



PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Docket No: Q78522

Jun FURUKAWA

Appln. No.: 10/718,663

Group Art Unit: 2131

Confirmation No.: 1253

Examiner: Unknown

Filed: November 24, 2003

For: WEAKLY COMPUTATIONAL ZERO-KNOWLEDGE PROOF AND EVALUATION

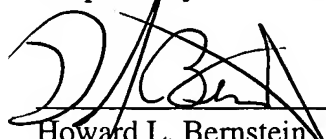
SUBMISSION OF PRIORITY DOCUMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Submitted herewith is a certified copy of the priority document on which a claim to priority was made under 35 U.S.C. § 119. The Examiner is respectfully requested to acknowledge receipt of said priority document.

Respectfully submitted,


Howard L. Bernstein
Registration No. 25,665

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE

23373

CUSTOMER NUMBER

Enclosures: JP 2002-341112

Date: April 29, 2004

US

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 2 年 1 1 月 2 5 日
Date of Application:

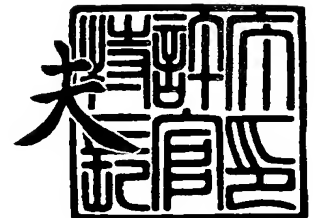
出 願 番 号 特 願 2 0 0 2 - 3 4 1 1 1 2
Application Number:
[ST. 10/C]: [J P 2 0 0 2 - 3 4 1 1 1 2]

出 願 人 日 本 電 気 株 式 有 限 公 司
Applicant(s):

2 0 0 3 年 8 月 2 2 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 3 - 3 0 6 9 1 0 0

【書類名】 特許願
【整理番号】 35001167
【あて先】 特許庁長官殿
【国際特許分類】 G09C 1/00

【発明者】

【住所又は居所】 東京都港区芝五丁目 7 番 1 号
本電気株式会社内

日

【氏名】 古川 潤

【特許出願人】

【識別番号】 000004237
【氏名又は名称】 日本電気株式会社

【代理人】

【識別番号】 100109313
【弁理士】
【氏名又は名称】 机 昌彦
【電話番号】 03-3454-1111

【選任した代理人】

【識別番号】 100085268
【弁理士】
【氏名又は名称】 河合 信明
【電話番号】 03-3454-1111

【選任した代理人】

【識別番号】 100111637
【弁理士】
【氏名又は名称】 谷澤 靖久
【電話番号】 03-3454-1111

【手数料の表示】

【予納台帳番号】 191928
【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0213988

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 証明システムと評価システム

【特許請求の範囲】

【請求項 1】 互いに通信が可能な生成装置と、証明装置と、検証装置と、からなり、証明装置は生成装置が生成した秘密事項である証拠を保有し、前記証拠を証明装置が保有することを検証装置が証明装置と対話することにより検証装置に証明する証明システムであって、

さらに、生成装置と、検証装置とそれぞれ通信可能な模擬装置と識別装置とを接続して前記証明システムを評価するとき、

前記各装置には、それぞれランダムなデータが記録されたランダムテープが入力され、

生成装置は、関係 R と共通入力からでは前記証拠を導出することが困難な数値上の前記関係 R を相互に有する前記共通入力と前記証拠とを前記関係 R をもとに前記ランダムテープから生成し、証明装置と識別装置には、生成された前記共通入力と前記証拠とを入力し、検証装置と模擬装置には、生成された前記共通入力を入力し、

検証装置は、前記共通入力と自身のランダムテープから入力したデータを使用して証明装置と対話することにより証明装置が前記証拠を有するか否かについての証明受理または証明拒絶を出力し、その結果、検証装置が入力したランダムテープのデータと証明装置との対話による対話データとを含む証明履歴を生成し、

模擬装置は、前記共通入力と自身に入力されるランダムテープを使用して検証装置にランダムテープを入力し検証装置と対話することで証明装置と検証装置による対話を証明装置を使用せずに模擬し、その結果、模擬装置が検証装置に入力したランダムテープのデータと模擬された対話データとを含む模擬証明履歴を生成し、

データの分布の相違を識別する識別装置は、生成装置から同じ前記共通入力を入力して生成された前記証明履歴と前記模擬証明履歴のデータの分布上の相違について、確率的に 1 に近似される大多数の前記共通入力の場合において、計算量理論的に識別不可能であり、かつ、確率的に無視できる少数の前記共通入力の場合

合においては、その相違を計算量理論的に識別可能であると評価することを特徴とする証明システム。

【請求項2】 互いに通信が可能な生成装置と、証明装置と、検証装置と、模擬装置と、識別装置と、からなり、証明装置は、生成装置が生成した秘密事項である証拠を保有し、証明装置が前記証拠を保有することを検証装置が証明装置と対話することにより検証装置に証明する証明システムを模擬装置と識別装置を前記証明システムに接続して評価する評価システムであって、前記各装置には、それぞれランダムなデータが記録されたランダムテープが入力され、

生成装置は、関係Rと共通入力からでは前記証拠を導出することが困難な数値上の前記関係Rを相互に有する前記共通入力と前記証拠とを前記関係Rをもとに前記ランダムテープから生成し、証明装置と識別装置には、生成された前記共通入力と前記証拠とを入力し、検証装置と模擬装置には、生成された前記共通入力を入力し、

検証装置は、前記共通入力と自身のランダムテープから入力したデータを使用して証明装置と対話することにより証明装置が前記証拠を有するか否かについての証明受理または証明拒絶を出力し、その結果、検証装置が入力したランダムテープのデータと証明装置との対話による対話データとを含む証明履歴を生成し、

模擬装置は、前記共通入力と自身に入力されるランダムテープを使用して検証装置にランダムテープを入力し検証装置と対話することで証明装置と検証装置による対話を証明装置を使用せずに模擬し、その結果、模擬装置が検証装置に入力したランダムテープのデータと模擬された対話データとを含む模擬証明履歴を生成し、

データの分布の相違を識別する識別装置は、同じ前記共通入力を入力して生成された前記証明履歴と前記模擬証明履歴のデータの分布上の相違について、確率的に1に近似される大多数の前記共通入力の場合において計算量理論的に識別不可能であるか否かの評価を行ない、評価と評価の根拠を評価結果として記憶装置に記憶するとともに、前記証明システムの前記評価結果を公開することを特徴とする評価システム。

【請求項 3】 互いに通信が可能な生成装置と、証明装置と、検証装置と、からなり、前記生成装置が生成した秘密事項である証拠を前記証明装置は保有し、前記証拠を証明装置が保有することを検証装置が証明装置と対話することにより検証装置に証明する証明システムであって、

さらに、生成装置と、検証装置と通信可能な模擬装置と識別装置とを接続して前記証明システムを評価するとき、

前記各装置には、それぞれランダムなデータが記録されたランダムテープが入力され、

生成装置は、関係 R と共通入力からでは前記証拠を導出することが困難な数値上の前記関係 R を相互に有する前記共通入力と前記証拠とを前記関係 R をもとに前記ランダムテープから生成し、証明装置と識別装置には、生成された前記共通入力と前記証拠とを入力し、検証装置と模擬装置には、生成された前記共通入力を入力し、

証明装置は、証明部とハッシュ部からなり、証明部は、検証装置またはハッシュ部にデータを送信し、ハッシュ部は、証明部から送られるデータのハッシュ値を計算して結果を証明部に返し、証明部とハッシュ部のデータの送受信により証明部とハッシュ部との対話データが生成され、前記対話データのうちハッシュ部から証明部に送られるデータをランダムなデータに変更した場合、ランダムなデータに変更された対話データと証明装置から検証装置に送付されるデータとからなる証明履歴と、

模擬装置は、証明装置と検証装置による対話を、証明装置を使用せず前記共通入力と自身に入力されるランダムテープとから模擬し、その結果、模擬された対話データを含む模擬証明履歴を生成し、

データの分布の相違を識別する識別装置は、生成装置から同じ前記共通入力を入力して生成された前記証明履歴と前記模擬証明履歴のデータの分布上の相違について、確率的に 1 に近似される大多数の前記共通入力の場合において、計算量理論的に識別不可能であり、かつ、確率的に無視できる少数の前記共通入力の場合においては、その相違を計算量理論的に識別可能である

と評価することを特徴とする証明システム。

【請求項4】 互いに通信が可能な生成装置と、証明装置と、検証装置と、模擬装置と、識別装置と、からなり、証明装置は、生成装置が生成した秘密事項である証拠を保有し、証明装置が前記証拠を保有することを検証装置が証明装置と対話することにより検証装置に証明する証明システムを模擬装置と識別装置を前記証明システムに接続して評価する評価システムであって、前記各装置には、それぞれランダムなデータが記録されたランダムテープが入力され、

生成装置は、関係Rと共通入力からでは前記証拠を導出することが困難な数値上の前記関係Rを相互に有する前記共通入力と前記証拠とを前記関係Rをもとに前記ランダムテープから生成し、証明装置と識別装置には、生成された前記共通入力と前記証拠とを入力し、検証装置と模擬装置には、生成された前記共通入力を入力し、

証明装置は、証明部とハッシュ部からなり、証明部は、検証装置またはハッシュ部にデータを送信し、ハッシュ部は、証明部から送られるデータのハッシュ値を計算して結果を証明部に返し、証明部とハッシュ部のデータの送受信により証明部とハッシュ部との対話データが生成され、前記対話データのうちハッシュ部から証明部に送られるデータをランダムなデータに変更した場合、ランダムなデータに変更された対話データと証明装置から検証装置に送付されるデータとからなる証明履歴と、

模擬装置は、証明装置と検証装置による対話を、証明装置を使用せず前記共通入力と自身に輸入されるランダムテープとから模擬し、その結果、模擬された対話データを含む模擬証明履歴を生成し、

データの分布の相違を識別する識別装置は、同じ前記共通入力を入力して生成された前記証明履歴と前記模擬証明履歴のデータの分布上の相違について、確率的に1に近似される大多数の前記共通入力の場合において計算量理論的に識別不可能であるか否かの評価を行ない、評価と評価の根拠を評価結果として記憶装置に記憶するとともに、前記証明システムの前記評価結果を公開することを特徴とする評価システム。

【請求項5】 請求項1または請求項3において、識別装置をどのような識

別装置に置き換えても、置き換えられた識別装置は、生成装置から同じ前記共通入力を入力して生成された前記証明履歴と前記模擬証明履歴のデータの分布上の相違について、確率的に 1 に近似される大多数の前記共通入力の場合において、計算量理論的に識別不可能であり、かつ、確率的に無視できる少数の前記共通入力の場合においては、その相違を計算量理論的に識別可能であると評価することを特徴とする証明システム。

【請求項 6】 請求項 2 または請求項 4 において、識別装置は、インターネットまたは電話回線を含むネットワークを通じて、前記証明システムの評価結果を送信することを特徴とする評価システム。

【請求項 7】 互いに通信が可能な生成装置と、証明装置と、検証装置と、からなり、証明装置は生成装置が生成した秘密事項である証拠を保有し、前記証拠を証明装置が保有することを検証装置が証明装置と対話することにより検証装置に証明するディフィーヘルマン事例でないことの証明システムであって、生成装置と証明装置と検証装置にそれぞれランダムなデータを記録したランダムテープと群を特定する値が入力され、生成装置は自身に入力されたランダムなデータから、前記群の要素 g 、 h 、 z' と整数 x を入力し、共通入力を g 、 h 、 $y = g^x$ 、 z' 、証拠を x として生成し、生成装置から証明装置に、前記共通入力と前記証拠を入力し、生成装置から前記検証装置に、前記共通入力を入力し、検証装置は、前記共通入力と自身のランダムテープから入力したデータを使用して証明装置と対話することによりその結果として証明装置が前記証拠を有するか否かについての証明受理または証明拒絶を出力するものであって、対話を開始した以降には、

(1) 検証装置は、ランダムテープから前記群の位数より小さい数である整数 b と、チャレンジ c とを無作為に選び、チャレンジコミットメント $a = g^{b y c}$ を生成し前記証明装置に送り、

(2) 証明装置は、ランダムテープを利用して前記群の位数より小さいある整数 d 、 e 、 f を一様無作為に選び、 $h' = h^d$ 、

$$w' = z' d、$$

$$v = h x d、$$

$$y' = g^e、$$

$$v' = h' e、$$

$$h'' = h f、$$

$$w'' = z' f \text{ を計算し、}$$

検証装置に h' 、 w' 、 v 、 y' 、 v' 、 h'' 、 w'' を送信し、

(3) 検証装置は前記整数 b 、 c を証明装置に送り、

(4) 証明装置は、受信した前記整数 b 、 c から $a = g^b y^c$ を確認し、この式が成り立たなかった場合は、プロトコルを中止し、成り立てば対話を続行し、

(5) 証明装置は、前記整数 d 、 e 、 f と前記証拠を用いて、レスポンス

$$r = x c + e \pmod{\text{群の位数}}、$$

$$r' = d c + f \pmod{\text{群の位数}} \text{ を計算して検証装置に送り、}$$

(6) 検証装置は、証明装置から受け取った前記 h' 、 w' 、 v 、 y' 、 v' 、 h'' 、 w'' と、前記 r 、 r' と、前記チャレンジ c 、前記共通入力 p 、 q 、 g 、 h 、 y 、 z' を用いて 4 個の等式と 1 個の不等式

$$g^r = y^c y'、$$

$$h^r = v^c v'、$$

$$h^{r'} = h'^c h''、$$

$$z'^{r'} = w'^c w''、$$

$$v \neq w' \pmod{p}$$

を確認し、全て成り立てば証明受理を、1 つでも成り立たなければ証明拒絶を出力する

ことを特徴とする証明システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

複数の装置が互いに通信することで証明及び検証を行うシステムで、そのシステムのある装置がもし規定にしたがって通信するならば、他のある装置に対して

秘密の情報を漏らさないことが保証されている通信による証明と検証の方法に関し、特にこのプロトコルが零知識証明クラスに属さない場合の証明システムと評価システムに関する。

【0 0 0 2】

【従来の技術】

従来の技術である零知識（ゼロ知識）証明クラスについて説明する。

【0 0 0 3】

零知識証明を解説した文献としては、例えば特許文献 1 と、非特許文献 1、非特許文献 2 がある。

【0 0 0 4】

公開鍵暗号、電子署名、相手認証、メッセージ認証、秘匿計算、電子現金等の、暗号技術を用いるプロトコルは、暗号プロトコルと呼ばれる。これらの暗号プロトコルは、通信内容を他人に漏らさない（公開鍵暗号）、本人以外は署名することができない（電子署名）、他人が成り済ますことができない（相手認証）、等の性質を満たすことが必須である。

【0 0 0 5】

これらの性質はいずれも、固有な情報を隠蔽する点において共通する特徴を持っている。例えば公開鍵暗号では暗号化のための秘密鍵が、電子署名では署名のための秘密鍵が、相手認証では本人を証明する秘密鍵が隠蔽される。

【0 0 0 6】

これらの暗号プロトコルにおいてはプロトコルの実行時に上記様々な秘密鍵が相手に漏れるようなことがあってはならない。そしてこのような秘密鍵が隠蔽されるという性質を暗号プロトコルが持つことを証明する方法に、暗号プロトコルが零知識証明クラスに属することを示すことによる方法がある。

【0 0 0 7】

およそ零知識証明クラスとは、秘密鍵等の秘密情報を有する証明者と証明者が秘密情報を有することを検証する検証者とからなる対話的な知識の証明プロトコル（証明者と検証者が互いに通信することで、証明者が検証者に何かを証明するプロトコル）全体の集合で、証明者が検証者に証明したいこと以外にいっさい情

報を漏らさないプロトコルの集合である。

【0 0 0 8】

これを相手認証の例を用いて説明する。

【0 0 0 9】

電子的な通信を通じて V（検証者）が P（証明者）を秘密情報を有する本人であると認証するには、P が V に、P しか持っていない秘密情報を持っていることを証明することでなし得る。しかし、もしここで P がその情報を V に渡すことによって情報の所持を証明したのならば、以降 V は P に成り済ますことができる。ところが、もしこの証明する方法（プロトコル）が零知識証明クラスに属するならば、P から V には、P が本人である証となる情報を持っているということ以外には伝わらないので、P は安心して V に証明してもらうことができる。

【0 0 1 0】

ある暗号プロトコルが零知識証明クラスに属することを証明するには、証明者と検証者の間で通信されるデータと「同様のデータ」を検証者自身が一人で生成できることを示せば良い（ここで言う「同様のデータ」の定義については後述）。

【0 0 1 1】

もしこのことが可能ならば、証明者との対話通信において検証者が獲得したデータ列は、もともと検証者が一人で生成し得たものであったので、検証者が自身で知り得ることができない証明者の秘密情報を知ろうとした時に、獲得したデータ列は何の役にも立たないことが分かる。それゆえ零知識証明クラスに属する暗号プロトコルは、証明者が検証者に証明したいことが真実かどうかという 1 ビットの情報以外にはいっさい情報を漏らさないことが保証される。

【0 0 1 2】

任意の対話的に証明可能な事柄を、零知識証明クラスに属する対話的な知識の証明プロトコルにて証明することは可能であるが、効率的な知識の証明システムを設計できるとは限らない。実際、零知識証明に属する効率的な証明システムを作るのが至難な証明対象は非常に多いことが問題となっている。

【0 0 1 3】

一方、零知識証明クラスに属する証明システムは余計な情報を漏らさないが、逆に、余計な情報を漏らさない証明システムは、零知識証明クラスに属するとは限らない。そこで、ある証明システムが、零知識証明クラスに属さなくとも、余計な情報を漏らさないクラスに属することを証明できるようになれば、暗号プロトコルの設計の自由度が増し、効率的な暗号プロトコルを作れる機会が増大すると思われる。

【0014】

まず、零知識証明クラスをより具体的に説明する。

【0015】

最初に対話的な知識の証明システムとは何かをより正確に説明する。

【0016】

対話的証明プロトコルには何らかの方法で互いに通信できる（対話できる）、証明者である証明装置Pと検証者である検証装置Vが登場する。

【0017】

あるデータXとW及び、関数 $R()$ があったとして、 $R(X, W) = 1$ としたとき、XとWは関係Rを満たすと呼び、 $(X, W) \in R$ と記述することにする。今XとW、 $R()$ が与えられれば、 $(X, W) \in R$ であることは計算機を用いてすぐに調べることができるが、Xと $R()$ だけが与えられた場合、これら与えられたX、 $R()$ に対して、 $(X, W) \in R$ なるWが何かは十分な時間をかけても分からないとする。

【0018】

この時XとWと $R()$ を知っている証明装置Pが、Xと $R()$ しか知らない検証装置Vに、与えられたX、 $R()$ に対して、 $(X, W) \in R$ なるWを証明装置Pが知っていることを互いに通信して納得させる方法を、対話的な知識の証明システムと呼ぶ。つまりPにWの知識（情報）があることを対話的に証明するプロトコルである。

【0019】

XからWを求めることが難しいものの具体的な例として、離散対数問題がある。pを大きな素数、gをpについての剰余類群 $(\mathbb{Z}/p\mathbb{Z})^*$ の元、wを $p-1$

についての剰余類群 $Z / (p - 1) Z$ の元、 $h = g^W \pmod{p}$ とする。

【0 0 2 0】

$X = \{p, g, h\}$ 、 $W = \{w\}$ とし、等式 $h = g^W \pmod{p}$ が成り立つなら X 、 W は関係 R を満たすとする。

【0 0 2 1】

この場合 X から W を求めることは、離散対数問題を解くことに当り、 p が大きい場合（例えば 1 0 0 0 ビット以上）一般には不可能とされている。実際単純に、 w として 1 から順番に $h = g^w \pmod{p}$ となるかを試していくと、平均して $p / 2$ 回の $g^w \pmod{p}$ を計算する必要がある。これはおよそ、延べ $p / 2$ 回の \pmod{p} 上の掛け算を実行せねばならない。 p が十分に大きいと、これは大変な事である。

【0 0 2 2】

一方、 $W (= w)$ が与えられた場合、等式 $h = g^W \pmod{p}$ を確認するのは簡単である。この計算は高々 $2 \log_2 p$ 回の \pmod{p} 上の掛け算を実行すれば終了する。 p が 1 0 2 4 b i t の時の例で言うと、 X から W を求めるには、2 1 0 2 3 回の乗算が必要で、 $(X, W) \in R$ を確認するには 2 0 4 8 (= 2 1 0) 回の乗算で済むことになる。

【0 0 2 3】

P が W を知っていることを V に納得させるもっとも簡単な方法は、 W を V に渡すことである。上の例の場合 P は V に w を渡す。

【0 0 2 4】

検証装置 V は等式 $h = g^W \pmod{p}$ を確認できれば納得するはずである。

【0 0 2 5】

しかし、本発明では W が検証装置 V に知られないような知識の証明方法に注目している。これが零知識証明クラス属する知識の証明システム、すなわち零知識証明である。

【0 0 2 6】

上に挙げた $(X, W) \in R$ の場合の零知識証明の例を挙げて、零知識証明を説

明していく。

【0027】

まず、証明装置 P と検証装置 V には、それぞれランダムテープと呼ばれる乱数の列からなるデータが個別に入力されるとする。P と V とには共通の入力として X も入力されている。共通の入力 X に対応して、X の証拠 W が証明装置 P に入力されているとする。今の場合 $X = \{p, g, h\}$ で、 $W = \{w\}$ である。

(1) 検証装置 V は、自身の持つランダムテープから

乱数 $b, c, \in \mathbb{Z} / (p-1)\mathbb{Z}$ を生成して、 $A = g^{b h^c} \bmod p$ を計

算し、証明装置 P に A を送る。

(2) 証明装置 P は自身の持つランダムテープから $s \in \mathbb{Z} / (p-1)\mathbb{Z}$

を生成して、 $B = g^s \bmod p$ を検証装置 V に送る。

(3) 検証装置 V は、A の生成に使用した b, c を証明装置 P に送る。

(4) 証明装置 P は、等式 $A = g^{b h^c} \bmod p$ が成り立つことを確認する。

【0028】

もし成り立たなければ、検証装置 V が不正を働いたと判断してここで終了する。成り立てば $r = c w + s \bmod p-1$ により生成した r を検証装置 V に送る。

(5) 検証装置 V は等式 $g^r = h^c B \bmod p$ が成り立つことを確認できれば、P は w を知っていると判断し、受理を出力する。成り立たなければ、不受理を出力する。

【0029】

上記知識の証明システムは以下の性質を満たす。

(1) 証明装置 P が w を知っていて P と V が上記手続きを正しく実行すれば、検証装置 V は受理を出力する。

(2) 証明装置 P が w を知らなければ、P が V をして受理を出力させる事は不可能である。

(3) 検証装置 V はプロトコルを通じて w に関する知識を得ることができない。

(1) の性質は、

$$g^r = g^{cw+s} \pmod{p} = g^{wc} g^s = h^{cB} \pmod{p}$$

より明らかである。

(2) の性質が成り立つことの厳密な証明は省略するが、証明装置 P が c を知ることになるのは、g、h、B が決定してからである。この時、どんな c を受け取っても等式 $g^r = h^{cB} \pmod{p}$ が成り立つような r を計算するには w の知識が不可欠であることが簡単に分かる。上記 (1)、(2) の性質を満たしていれば、この上記プロトコルは零知識の証明システムである。

【0030】

次に (3) の性質についてであるが、上記プロトコルを通じて検証装置 V が得たデータは、検証装置 V のランダムテープ、A、B、b、c、r だけである。p、g、h は最初から持っていた。もし、この検証装置 V の持つランダムテープと、A、B、b、c、r のデータを、証明装置 P と通信せずに同様のものを自分で産み出せるならば、検証装置 V は証明装置 P からプロトコルを通じて得た知識はないと言える。

【0031】

以下に、証明システムを証明装置 P を使用しない形で模擬する模擬装置 S が、検証装置 V を使ってこのようなデータを作る方法を示す。模擬装置 S にはランダムテープが入力されるとする。

- (1) まず、模擬装置 S のランダムテープで、検証装置 V のランダムテープを一樣無作為に決め、これを検証装置 V に入力する。
- (2) すると、検証装置 V は A を出力する。
- (3) 模擬装置 S はランダムに B を選んで検証装置 V に入力する。
- (4) すると、検証装置 V は b、c を出力する。
- (5) 模擬装置 S は、ここで一旦検証装置 V の電源を落す等によって、検証装置 V を初期状態にリセットする。
- (6) 模擬装置 S は、再度、検証装置 V を立ち上げ、先と同じ同じランダムテープからのデータを検証装置 V に入力する。
- (7) すると、検証装置 V は前回と同じ A を出力する。

(8) 模擬装置 S はランダムに r を選び、

$B = g^{r h^{-c}} \bmod p$ を計算し、 B を検証装置 V に入力する。

(9) 検証装置 V は前回と同じ b 、 c を出力する。

(10) そこで、模擬装置 S は r を検証装置 V に入力する。

(11) すると、検証装置 V は受理を出力する。

【0032】

このようにして模擬装置 S により生成された V のランダムテープと A 、 B 、 b 、 c 、 r からなる集合の最終的な分布は、検証装置 V が証明装置 P と通信して得られる集合の分布と全く同じになる。模擬装置 S は検証装置 V にデータを入力してその出力を得ているだけなので、検証装置 V の構造がどうなっているかも解析するさえ必要がない。

【0033】

模擬装置 S が検証装置 V を使って生成したデータの分布と証明装置 P と検証装置 V の通信によって得られるデータの分布が全く同じことを以下に示す。

【0034】

まず、ランダムテープは全くランダムな分布を持っているものとする。証明装置 P と検証装置 V の通信によって得られる B はその生成方法から全くランダムに分布する。(s を $\mathbb{Z}/(p-1)\mathbb{Z}$ から生成して、 $B = g^s \bmod p$ としているから。)

A 、 b 、 c は検証装置 V によって決定されるので、この分布は検証装置 V による。これらの値が決定したら、自動的に r の値は決定される。

【0035】

模擬装置 S から得られる r はその生成方法から全くランダムに分布する。 A 、 b 、 c は検証装置 V に生成させたので、証明装置 P が検証装置 V と通信して生成する場合と全く同じ分布で生成される。これらの値が決定したら、自動的に B の値は決定される。 r をランダムに分布させ r によって B を決定した時の r 、 B の分布と、 B をランダムに分布させ B によって r を決定した時の r 、 B の分布は同じである。よって、両者の分布は同じである。

【0036】

すなわち、証明装置 P と検証装置 V による真のプロトコルから得られるデータ列も、模擬装置 S が生成するデータ列も、同じ分布から一様無作為に抽出したデータ列といえる。

【0037】

これは検証装置 V がわざわざ証明装置 P と通信せずとも、勝手に自分で同じデータを作れる、すなわち、検証装置 V は、元々単独で計算可能な情報しか証明装置 P から抽出できないということである。このような議論から性質 3 が証明できたことになる。

【0038】

ここで零知識証明をより一般化して記述する。

【0039】

証明装置 P は検証装置 V に $(X, W) \in R$ なる W の知識を持っていることを証明するとする。P と V とで互いに交換されるデータを通信される順番に $m_1, m'_1, m_2, m'_2, \dots, m_k, m'_k$ とする。

【0040】

m_1, \dots, m_k は、検証装置 V から証明装置 P へ送られるデータとし、 m'_1, \dots, m'_k は、証明装置 P から検証装置 V へ送られるデータとする。また検証装置 V に入力されるランダムテープをランダムテープ r_V 、証明装置 P に入力されるランダムテープをランダムテープ r_P とする。

【0041】

固定された X, W に対して、 r_P, r_V を決めると、 $m_1, m'_1, m_2, m'_2, \dots, m_k, m'_k$ が得られる。ここで固定された X, W と一様無作為に選ばれる r_P, r_V に対する $m_1, m'_1, m_2, m'_2, \dots, m_k, m'_k, r_V$ の分布を考える。（ここで r_V の分布は V が自由に決めて良い。）

この分布は W を知っている P の助けを借りて生成されるものであるが、この分布が、もしあるランダムテープ s_V の入力される模擬装置 S が存在して、検証装置 V が証明装置 P といっさい通信せずに、模擬装置 S の助けを借りて生成する $n_1, n'_1, n_2, n'_2, \dots, n_k, n'_k, r_V$ からなる固定された X, W と一様無作為に選ばれる s_V, r_V に対する分布との見分けがつかないの



ならば、証明装置 P と検証装置 V の相互通信による W を知っていることの証明は零知識証明クラスに属しているという。

【0042】

ここで模擬装置 S には W は入力されていない。検証装置 V が証明装置 P と通信することにより得られるデータ列 $m_1, m'_1, m_2, m'_2, \dots, m_k, m'_k, r_V$ は、検証装置 V にとって証明装置 P と通信せずに生成できるデータ列と同等のものであるから、検証装置 V は証明装置 P との通信によって何ら有益な情報を得ることができないと言える。

【0043】

ここで言う二つの分布が見分けがつかないとはどういうことか説明する。

【0044】

二つの分布の識別を行う識別装置 D は、乱数列からなる識別装置 D のもつランダムテープ r_D および $m_1, m'_1, m_2, m'_2, \dots, m_k, m'_k, r_V$ と、数列 $n_1, n'_1, n_2, n'_2, \dots, n_k, n'_k, r_V$ が入力されてその識別した真／模擬の結果として 1 または 0 を出力するとする。

【0045】

定められたランダムテープ r_P, r_V, r_D の分布から一様無作為に r_P, r_V, r_D を選んだときに、数列 $m_1, m'_1, m_2, m'_2, \dots, m_k, m'_k, r_V$ が入力された識別装置 D が 1 を出力する確率を、

$$\Pr_{\{r_P, r_V, r_D\}} [D(m_1, \dots, m'_k, r_V) = 1]$$
 と記す。

【0046】

定められたランダムテープ r_S, r_D の分布から一様無作為に r_S, r_D を選んだときに、数列 $n_1, n'_1, n_2, n'_2, \dots, n_k, n'_k, r_V$ が入力された識別装置 D が 1 を出力する確率を、

$$\Pr_{\{r_S, r_D\}} [D(n_1, \dots, n'_k, r_V) = 1]$$
 と記す。

【0047】

この時どのような識別装置 D を用いても、

$$\Pr_{\{r_P, r_V, r_D\}} [D(m_1, \dots, m'_k, r_V) = 1]$$
 と、

$P \text{ } _ \{ \{rS, rD\} \mid [D(n_1, \dots, n'_k, rV) = 1] \}$ の差が無視できるほど小さければ、二つの分布は見分けがつかないという。

【0048】

ある証明システムが零知識証明クラスに属するためには、証明装置 P と検証装置 V に共通に与えられた共通入力 X 及びそれに関係 R で対応する W に対して、模擬装置 S が存在して、どのような識別装置 D にも、模擬装置 S が生成するデータ列と、真のデータ列を区別できない必要があった。

【0049】

固定された X と W に対して、どのような識別装置 D とされているので、識別装置 D はデータ W を所持しているようなものや、証明装置 P すら知らない X と W に関わる情報を持つ装置も含むため、この零知識クラスに属するための制約条件は、大変きつい。

【0050】

実際、証明装置 P が X と W の組を生成するとして、 $(X, W) \in R$ となるよう一様無作為に X、W を生成しなければ、W を検証装置 V に推測される可能性がある。もちろん一様無作為に選んでも、検証装置 V が、たまたま試してみた W が的中する可能性もある。よって、入力されたランダムテープから X、W を生成する生成装置 G を考えたとき、大多数のランダムテープが選ばれた場合にのみ検証装置 V は W を知ることができないのであって、無視できるほど低い確率においては、検証装置 V は W を知ることができる。

【0051】

このように、生成装置 G に入力されるランダムテープの大多数の場合に関して W が漏れるかどうかを考えることが自然であると思われる。

[正直な検証者の零知識証明クラス]

今まで考えてきた零知識証明クラスは、どのような悪質な検証装置 V に対しても証明装置 P から W に関する知識が漏れないことを前提にしたものであった。しかし、定められた通りに動作する信頼のできる検証装置 V を考えることが有用な場合がある。特に検証装置 V から証明装置 P へ送られるデータが乱数のみの場合は特に有効である。

【0052】

前述した例で検証装置Vが $A = g^b h^c \bmod p$ を証明装置Pへ送った後に、証明装置PがBを送っているのはcをBに依存して検証装置Vによって恣意的に選ばれることを防ぐためである。

【0053】

もし検証装置Vが正直にcを一様無作為に選ぶならば、前述の例は以下のように単純化される。

- (1) 証明装置Pはランダムテープから $s \in \mathbb{Z} / (p-1)\mathbb{Z}$ を生成して、 $B = g^s \bmod p$ を生成して検証装置Vに送る。
- (2) 検証装置Vは一様無作為に選んだcをPに送る。
- (3) 証明装置Pは、 $r = cw + s \bmod p-1$ をVに送る。
- (4) 検証装置Vは、等式 $g^r = h^c B \bmod p$ が成り立つことが確認できれば

ば、Pはwを知っていると判断し、受理を出力する。成り立たなければ、不受理を出力する。

【0054】

模擬装置SがB、c、rと同様のデータ列を作る方法は以下の通りである。

【0055】

模擬装置Sは、一様無作為にc、rを選んで、 $B = g^r h^{-c} \bmod p$ とする。

【0056】

上記の単純化はシステムの簡略化以上の効果がある。ここで、検証装置VがBを入力された` `後に` `ランダムにcを選ぶことが本質なのである。

【0057】

証明装置Pが 検証装置Vの代わりに暗号学的なハッシュ関数 $Hash()$ を用いて、

$c = Hash(B, p, g, h)$ と自らcを生成しても同様の安全性が得られると考えられる。

【0058】

証明装置 P は c を選ぶことはほとんど不可能なので、やはり w を知らないで検証を通過することが出来る r を生成することができないのである。このハッシュ関数を導入したプロトコルを書き下してみると、

(1) 証明装置 P はランダムテープから $s \in \mathbb{Z} / (p-1)\mathbb{Z}$ を生成して、

$$B = g^s \bmod p, \quad c = \text{Hash}(p, g, h, B), \\ r = cw + s \bmod p-1 \text{ とする。}$$

(3) 証明装置 P は B, r を検証装置 V に送る。

(4) 検証装置 V は $c' = \text{Hash}(p, g, h, B)$ とし、

等式 $g^r = h^{c'} B \bmod p$ が成り立つことが確認できれば、P は w を

知っているとは判断し、受理を出力する。成り立たなければ、不受理を出力する。

【0059】

この改良システムでは、検証装置 V から証明装置 P にデータを送信する必要がなくなった。よって証明装置 P は、 B, r を作成して検証装置に送付してしまえば誰にでも検証可能である。そのため、署名や暗号といったものにも応用することができる。

【0060】

ハッシュ関数を用いた零知識証明を用いると証明は次のようにして実現できる。

【0061】

文章 M からハッシュ関数を用いて $(\mathbb{Z} / p\mathbb{Z})^*$ の元 g に落す。ここで $g = \text{Hash}(M)$ であるが、このハッシュ関数の使用は、前述の零知識証明とは直接は関係ない。次に $h = g^w \bmod p$ とし、 w を知っていることの零知識証明を B, r を生成する。 M に h, B, r を証明として添付する。署名の検証者は M から g を、 p, h, g, B から c を再現し、等式 $g^r = h^{c'} B \bmod p$ が成り立つことを確認すればよい。

【0062】

【特許文献 1】

特開 2001-251289 (第 12-29 頁、図 1)

【非特許文献 1】

岡本龍明、山本博資著、産業図書出版「現代暗号」131-150頁

【非特許文献 2】

オデッド・ゴルドライツヒ著、ケンブリッジ出版の「ファウンデーション・オブ・クリプトグラフィー」(Oded Goldreich, Cambridge, 「Foundation of Cryptography」)184-330頁

【0063】

【発明が解決しようとする課題】

余計な情報を漏らさないことが保証された証明システムを作成するには、従来は零知識証明クラスに属するよう証明システムを作成する必要があった。ところが、このようにして証明システムの作成を試みた場合、必ずしも効率の良い証明システムを作成できるとは限らなかった。

【0064】

本発明はこのような状況を鑑みてなされたものである。

【0065】

本発明では、零知識証明クラスよりも広いクラスに対しても余計な情報を漏らさないことを保証する方法を与える。これにより、余計な情報を漏らさない証明システムの設計の幅を大きくし、今までは作ることのできなかった効率が良くかつ余計な情報を漏らさないことが保証されたプロトコルを、新たに作成する方法を与えることが可能となる。

【0066】

証明システムが零知識証明クラスに属するためには、与えられた証明装置と検証装置の共通した入力に対して、ある模擬装置が存在していかなる識別装置も証明装置と検証装置との対話による真の証明から得られるデータと、模擬装置から得られるデータが区別できないという条件を満たさねばならなかった。

【0067】

本発明ではこれを、証明装置と検証装置に対する共通した入力と証明装置への証拠を生成する生成装置のランダムテープの大多数の事例においてのみ、ある模

擬装置が存在して、証明装置にのみ入力される証拠を入力されたいかなる識別装置も、証明装置と検証装置との対話による真の証明から得られるデータと、模擬装置から得られるデータとの相違が、区別できなければ良いとして零知識証明クラスの条件を緩和する。

【0068】

この緩和された証明システムも余計な情報を漏らさないシステムであることが保証される。この緩和されたクラスのことを弱計算量的零知識証明クラスと呼ぶ。

【0069】

本発明は、この弱計算量的零知識証明クラスに属する証明システムを用いることによって、高速である等従来と異なる特徴を持つとともに、従来どうり余計な情報を漏らさないことを保証して、証明装置が検証装置に秘密の知識の所持を証明する事を可能とする証明システムと評価システムを提供するものである。

【0070】

【課題を解決するための手段】

本発明の第1の証明システムは、互いに通信が可能な生成装置と、証明装置と、検証装置と、からなり、証明装置は生成装置が生成した秘密事項である証拠を保有し、前記証拠を証明装置が保有することを検証装置が証明装置と対話することにより検証装置に証明する証明システムであって、

さらに、生成装置と、検証装置とそれぞれ通信可能な模擬装置と識別装置とを接続して前記証明システムを評価するとき、

前記各装置には、それぞれランダムなデータが記録されたランダムテープが入力され、

生成装置は、関係Rと共通入力からでは前記証拠を導出することが困難な数値上の前記関係Rを相互に有する前記共通入力と前記証拠とを前記関係Rをもとに前記ランダムテープから生成し、証明装置と識別装置には、生成された前記共通入力と前記証拠とを入力し、検証装置と模擬装置には、生成された前記共通入力を入力し、

検証装置は、前記共通入力と自身のランダムテープから入力したデータを使用し

て証明装置と対話することにより証明装置が前記証拠を有するか否かについての証明受理または証明拒絶を出力し、その結果、検証装置が入力したランダムテープのデータと証明装置との対話による対話データとを含む証明履歴を生成し、模擬装置は、前記共通入力と自身に入力されるランダムテープを使用して検証装置にランダムテープを入力し検証装置と対話することで証明装置と検証装置による対話を証明装置を使用せずに模擬し、その結果、模擬装置が検証装置に入力したランダムテープのデータと模擬された対話データとを含む模擬証明履歴を生成し、

データの分布の相違を識別する識別装置は、生成装置から同じ前記共通入力を入力して生成された前記証明履歴と前記模擬証明履歴のデータの分布上の相違について、確率的に1に近似される大多数の前記共通入力の場合において、計算量理論的に識別不可能であり、かつ、確率的に無視できる少数の前記共通入力の場合においては、その相違を計算量理論的に識別可能であると評価することを備える。

【0071】

本発明の第2の評価システムは、互いに通信が可能な生成装置と、証明装置と、検証装置と、模擬装置と、識別装置と、からなり、証明装置は、生成装置が生成した秘密事項である証拠を保有し、証明装置が前記証拠を保有することを検証装置が証明装置と対話することにより検証装置に証明する証明システムを模擬装置と識別装置を前記証明システムに接続して評価する評価システムであって、前記各装置には、それぞれランダムなデータが記録されたランダムテープが入力され、

生成装置は、関係Rと共通入力からでは前記証拠を導出することが困難な数値上の前記関係Rを相互に有する前記共通入力と前記証拠とを前記関係Rをもとに前記ランダムテープから生成し、証明装置と識別装置には、生成された前記共通入力と前記証拠とを入力し、検証装置と模擬装置には、生成された前記共通入力を入力し、

検証装置は、前記共通入力と自身のランダムテープから入力したデータを使用して証明装置と対話することにより証明装置が前記証拠を有するか否かについての

証明受理または証明拒絶を出力し、その結果、検証装置が入力したランダムテープのデータと証明装置との対話による対話データとを含む証明履歴を生成し、

模擬装置は、前記共通入力と自身に入力されるランダムテープを使用して検証装置にランダムテープを入力し検証装置と対話することで証明装置と検証装置による対話を証明装置を使用せずに模擬し、その結果、模擬装置が検証装置に入力したランダムテープのデータと模擬された対話データとを含む模擬証明履歴を生成し、

データの分布の相違を識別する識別装置は、同じ前記共通入力を入力して生成された前記証明履歴と前記模擬証明履歴のデータの分布上の相違について、確率的に 1 に近似される大多数の前記共通入力の場合において計算量理論的に識別不可能であるか否かの評価を行ない、評価と評価の根拠を評価結果として記憶装置に記憶するとともに、前記証明システムの前記評価結果を公開することを備える。

【0072】

本発明の第3の証明システムは、互いに通信が可能な生成装置と、証明装置と、検証装置と、からなり、前記生成装置が生成した秘密事項である証拠を前記証明装置は保有し、前記証拠を証明装置が保有することを検証装置が証明装置と対話することにより検証装置に証明する証明システムであって、

さらに、生成装置と、検証装置と通信可能な模擬装置と識別装置とを接続して前記証明システムを評価するとき、

前記各装置には、それぞれランダムなデータが記録されたランダムテープが入力され、

生成装置は、関係Rと共通入力からでは前記証拠を導出することが困難な数値上の前記関係Rを相互に有する前記共通入力と前記証拠とを前記関係Rをもとに前記ランダムテープから生成し、証明装置と識別装置には、生成された前記共通入力と前記証拠とを入力し、検証装置と模擬装置には、生成された前記共通入力を入力し、

証明装置は、証明部とハッシュ部からなり、証明部は、検証装置またはハッシュ部にデータを送信し、ハッシュ部は、証明部から送られるデータのハッシュ値を

計算して結果を証明部に返し、証明部とハッシュ部のデータの送受信により証明部とハッシュ部との対話データが生成され、前記対話データのうちハッシュ部から証明部に送られるデータをランダムなデータに変更した場合、ランダムなデータに変更された対話データと証明装置から検証装置に送付されるデータとからなる証明履歴と、

模擬装置は、証明装置と検証装置による対話を、証明装置を使用せず前記共通入力と自身に入力されるランダムテープとから模擬し、その結果、模擬された対話データを含む模擬証明履歴を生成し、

データの分布の相違を識別する識別装置は、生成装置から同じ前記共通入力を入力して生成された前記証明履歴と前記模擬証明履歴のデータの分布上の相違について、確率的に 1 に近似される大多数の前記共通入力の場合において、計算量理論的に識別不可能であり、かつ、確率的に無視できる少数の前記共通入力の場合においては、その相違を計算量理論的に識別可能であると評価することを備える。

【 0 0 7 3 】

本発明の第 4 の評価システムは、互いに通信が可能な生成装置と、証明装置と、検証装置と、模擬装置と、識別装置と、からなり、証明装置は、生成装置が生成した秘密事項である証拠を保有し、証明装置が前記証拠を保有することを検証装置が証明装置と対話することにより検証装置に証明する証明システムを模擬装置と識別装置を前記証明システムに接続して評価する評価システムであって、前記各装置には、それぞれランダムなデータが記録されたランダムテープが入力され、

生成装置は、関係 R と共通入力からでは前記証拠を導出することが困難な数値上の前記関係 R を相互に有する前記共通入力と前記証拠とを前記関係 R をもとに前記ランダムテープから生成し、証明装置と識別装置には、生成された前記共通入力と前記証拠とを入力し、検証装置と模擬装置には、生成された前記共通入力を入力し、

証明装置は、証明部とハッシュ部からなり、証明部は、検証装置またはハッシュ部にデータを送信し、ハッシュ部は、証明部から送られるデータのハッシュ値を

計算して結果を証明部に返し、証明部とハッシュ部のデータの送受信により証明部とハッシュ部との対話データが生成され、前記対話データのうちハッシュ部から証明部に送られるデータをランダムなデータに変更した場合、ランダムなデータに変更された対話データと証明装置から検証装置に送付されるデータとからなる証明履歴と、

模擬装置は、証明装置と検証装置による対話を、証明装置を使用せず前記共通入力と自身に入力されるランダムテープとから模擬し、その結果、模擬された対話データを含む模擬証明履歴を生成し、

データの分布の相違を識別する識別装置は、同じ前記共通入力を入力して生成された前記証明履歴と前記模擬証明履歴のデータの分布上の相違について、確率的に 1 に近似される大多数の前記共通入力の場合において計算量理論的に識別不可能であるか否かの評価を行ない、評価と評価の根拠を評価結果として記憶装置に記憶するとともに、前記証明システムの前記評価結果を公開することを備える。

【0074】

本発明の第 5 の証明システムは、第 1 または第 3 の発明において、識別装置をどのような識別装置に置き換えても、置き換えられた識別装置は、生成装置から同じ前記共通入力を入力して生成された前記証明履歴と前記模擬証明履歴のデータの分布上の相違について、確率的に 1 に近似される大多数の前記共通入力の場合において、計算量理論的に識別不可能であり、かつ、確率的に無視できる少数の前記共通入力の場合においては、その相違を計算量理論的に識別可能であると評価することを備える。

【0075】

本発明の第 6 の評価システムは、第 2 または第 4 の発明において、識別装置は、インターネットまたは電話回線を含むネットワークを通じて、前記証明システムの評価結果を送信することを備える。

【0076】

本発明の第 7 の証明システムは、互いに通信が可能な生成装置と、証明装置と

、検証装置と、からなり、証明装置は生成装置が生成した秘密事項である証拠を保有し、前記証拠を証明装置が保有することを検証装置が証明装置と対話することにより検証装置に証明するディフィーヘルマン事例でないことの証明システムであって、

生成装置と証明装置と検証装置にそれぞれランダムなデータを記録したランダムテープと群を特定する値が入力され、

生成装置は自身に入力されたランダムなデータから、前記群の要素 g 、 h 、 z' と整数 x を入力し、共通入力を g 、 h 、 $y = g^x$ 、 z' 、証拠を x として生成し、生成装置から証明装置に、前記共通入力と前記証拠を入力し、

生成装置から前記検証装置に、前記共通入力を入力し、

検証装置は、前記共通入力と自身のランダムテープから入力したデータを使用して証明装置と対話することによりその結果として証明装置が前記証拠を有するか否かについての証明受理または証明拒絶を出力するものであって、

対話を開始した以降には、

(1) 検証装置は、ランダムテープから前記群の位数より小さい数である整数 b と、チャレンジ c とを無作為に選び、チャレンジコミットメント $a = g^{b y c}$ を生成し前記証明装置に送り、

(2) 証明装置は、ランダムテープを利用して前記群の位数より小さいある整数 d 、 e 、 f を一様無作為に選び、

$$h' = h^d、$$

$$w' = z'^d、$$

$$v = h^{x d}、$$

$$y' = g^e、$$

$$v' = h'^e、$$

$$h'' = h^f、$$

$$w'' = z'^f \text{ を計算し、}$$

検証装置に h' 、 w' 、 v 、 y' 、 v' 、 h'' 、 w'' を送信し、

(3) 検証装置は前記整数 b 、 c を証明装置に送り、

(4) 証明装置は、受信した前記整数 b 、 c から $a = g^{b y c}$ を確認し、この式

が成り立たなかった場合は、プロトコルを中止し、成り立てば対話を続行し、

(5) 証明装置は、前記整数 d 、 e 、 f と前記証拠を用いて、レスポンス

$$r = x \cdot c + e \pmod{\text{群の位数}},$$

$$r' = d \cdot c + f \pmod{\text{群の位数}} \text{ を計算して検証装置に送り、}$$

(6) 検証装置は、証明装置から受け取った前記 h' 、 w' 、 v 、 y' 、 v' 、 h'' 、 w'' と、前記 r 、 r' と、前記チャレンジ c 、前記共通入力 p 、 q 、 g 、 h 、 y 、 z' を用いて 4 個の等式と 1 個の不等式

$$g^r = y^c \cdot y',$$

$$h' \cdot r = v^c \cdot v',$$

$$h \cdot r' = h' \cdot c \cdot h'',$$

$$z' \cdot r' = w' \cdot c \cdot w'',$$

$$v \neq w' \pmod{p}$$

を確認し、全て成り立てば証明受理を、1 つでも成り立たなければ証明拒絶を出力する

ことを備える。

【0077】

【発明の実施の形態】

最初に本発明の概要を簡単に説明する。

【0078】

あるデータ X と W 及び、関数 $R()$ があったとして、 $R(X, W) = 1$ としたとき、 X と W は関係 R を満たすと呼び、 $(X, W) \in R$ と記述することにする。

【0079】

本発明は、 $(X, W) \in R$ なる W なる秘密事項を証明装置が知っていることを検証装置によって検証する証明システムに関するものであり、さらに、証明装置の持つ W に関する情報を証明装置以外には何も漏らさないことを保証したまま証明する証明システムに関し、従来の零知識証明システムを発展させた内容を持つものである。これを弱計算量的零知識証明クラスに属する証明システムと呼ぶ。

【0080】

ある証明システムの属する証明クラスが、本発明の弱計算量的零知識証明クラ

スに属するものであるかを評価するため、証明装置と検証装置との間の証明プロトコルを模擬する模擬装置を評価の対象とする証明システムに接続して模擬装置による模擬された結果としての模擬データを生成する。

【0081】

さらに識別装置を接続して、この識別装置が、模擬データと、証明装置と検証装置の証明プロトコルによって生成される真のデータと、を比較することで証明システムが本発明における弱計算量的零知識証明クラスに属するかを判定する内容を持つものである。

【0082】

本発明の第1の実施の形態について図面を参照して説明する。

【0083】

本発明の第1の実施の形態の構成は、図1を参照すると、生成装置100と、Wという証拠（秘密事項）を所持する証明装置105と、証明装置105が証拠を保持することを検証する検証装置106と、からなる。

【0084】

生成装置100は、複数の乱数を記憶するランダムテープ $rG101$ と生成装置100以外の装置によって決定される固定データ102とが与えられたら、固定データ102をもとに、一様無作為に証拠103を選び、次に $(X, W) \in R$ となるような共通入力104を一様無作為に生成する。固定データ102は、関係Rを生成するための前提となる条件を与える。

【0085】

尚、固定データの一例としては、大きな素数 p 、 q があり、 q は $p-1$ を割るような関係を持つものがある。

【0086】

さらに、 X, W, R () の一例としては、従来の技術に記載したように、離散対数の関係がある。このとき、 p を大きな素数、 g を p についての既約剰余類 $(\mathbb{Z}/p\mathbb{Z})^*$ の元、 w を $p-1$ についての剰余類 $\mathbb{Z}/(p-1)\mathbb{Z}$ の元、 $h = g^w \pmod{p}$ とする。 $X = \{p, g, h\}$ 、 $W = \{w\}$ とし、等式 $h = g^w \pmod{p}$ が成り立つなら X, W は関係Rを満たすとするよ

うな例がある。

【0087】

生成装置100が固定データ102から生成した共通入力104は、証明装置105と検証装置106に入力され、証拠103は証明装置105にのみ入力される。共通入力104を証明装置105と検証装置106への共通の入力のため共通入力104と呼ぶことにする。

【0088】

生成装置100と、証明装置105と、検証装置106と、以降説明する模擬装置110と、識別装置112とは、それぞれ乱数を記録するランダムテープを含むデータに対する処理を行うCPUや主記憶メモリや、二次記憶装置である磁気ディスク装置、磁気テープ装置等を有するコンピュータであって、以下の実施の形態や実施例で説明される処理内容は、全て当該するコンピュータ上で動作するプログラムによって実行されている。

【0089】

また、生成装置100と、証明装置105と、検証装置106と、模擬装置110と、識別装置112は、それぞれイーサネット（登録商標）やインターネット等の通信手段によって接続され、相互にデータの送受信が可能であるとする。また、乱数を記憶したランダムテープは、二次記憶装置上のファイルとする。

【0090】

今、証明装置105と検証装置106とで互いに交換される対話データ107を通信される順番に m_1 、 m'_1 、 m_2 、 m'_2 、 \dots 、 m_k 、 m'_k とする。

【0091】

m_1 、 \dots 、 m_k は検証装置106から証明装置105へ送られるデータとし、 m'_1 、 \dots 、 m'_k は証明装置105から検証装置106へ送られるデータとする。

【0092】

また、検証装置106に入力される複数個の乱数を記録したランダムテープをランダムテープrV108、証明装置105に入力される複数個の乱数を記録す

るランダムテープをランダムテープ $rP109$ とする。

【0093】

ランダムテープ $rG101$ 、 $rP109$ 、 $rV108$ を決めると対話データ 107 が決まる。

【0094】

ここで一様無作為に乱数が選ばれる生成装置 100 のランダムテープ $rG101$ と、 $rP109$ と、 $rV108$ によって決定された対話データ 107 の m_1 、 m'_1 、 m_2 、 m'_2 、 \dots 、 m_k 、 m'_k と、ランダムテープ $rV108$ とからなる分布を考える。（ここでランダムテープ rV の分布は検証装置 $V106$ が自由に決めて良い。）

尚、ランダムテープ $rG101$ による共通入力 104 と対話データ 107 とランダムテープ $rV108$ とから生成されたデータを併せて証明履歴 111 と呼ぶ。

【0095】

この分布は、証拠 103 を知っている証明装置 105 の助けを借りて生成されるものである。この証明システムのプロトコルを模擬するある模擬装置 110 が存在するとする。

【0096】

この分布が、模擬装置 110 が証明装置 105 といっさい通信せずに検証装置 106 の助けを借りて生成する模擬された模擬証明履歴 115 である数値の列 n_1 、 n'_1 、 n_2 、 n'_2 、 \dots 、 n_k 、 n'_k 、 rV の、生成装置 100 、模擬装置 110 のランダムテープ rV 、 rS についての分布と、その分布の相違を識別するどのような識別装置 112 にも識別できないのならば、証明装置 105 と検証装置 106 の相互通信による共通入力 104 に対応する証拠 103 を知っていることの証明は、弱計算量的零知識証明クラスに属していると呼ぶ事にする。

【0097】

このような弱計算量的零知識証明クラスに属する証明システムを使って知識の証明をすることが、本実施の形態の内容である。

<検証者単独でのプロトコル再現装置の構成方法>

証明システムのプロトコルの模擬をする装置を模擬装置 110 とする。模擬装置 110 には乱数からなるランダムテープ $rS114$ が入力される。模擬装置 110 は、検証装置 106 をリセットして再立ち上げ可能な形で検証装置 106 と接続する。

【0098】

検証装置 106 に入力されるランダムテープ $rV113$ は、ランダムテープ $rS114$ から生成され、模擬装置 110 から検証装置 106 に入力される。

【0099】

検証装置 106 には証明装置 105 と検証装置 106 の共通入力 104 が入力される。模擬装置 110 はランダムテープ $rV113$ を検証装置 106 に入力し、それに対して検証装置 106 は n_1 を出力する。

【0100】

次に、模擬装置 110 はランダムテープ $rS114$ を用いて、 n'_1 を生成し、検証装置 106 に入力する。このように模擬装置 110 と検証装置 106 とで検証装置 106 が停止するか不受理を出力するまで証明プロトコルを行うことにより、適当な対話数 L までの n_1 、 n'_1 、 n_2 、 n'_2 、 \dots 、 n_L を得ることができる。

【0101】

検証装置 106 が停止するか不受理を出力するまでのこれらの値から模擬装置 110 は、検証装置 106 が何を出力するかを調べた後、検証装置 106 をリセットする等によって最初から模擬装置 110 と検証装置 106 の証明プロトコルを実行し直す。

【0102】

この時、模擬装置 110 は、検証装置 106 に前回と同じランダムテープ $rV113$ を入力する。模擬装置 110 は、検証装置 106 の今回の出力と前回の出力の相違を、模擬装置 110 から検証装置 106 へ入力する数値列 n_1 、 n'_1 、 n_2 、 n'_2 、 \dots 、 n'_{L-1} の相違に起因するものだけとする。

【0103】

また、前回の検証装置 106 の出力のデータを知ることが出来たため、模擬装置 110 は検証装置 106 へ入力する n_1 、 n'_1 、 n_2 、 n'_2 、 \dots 、 n_{L-1} の値を、検証装置 106 が証明プロトコルを受理する可能性が高いものを選ぶようにする。

【0104】

このような、証明プロトコルの中断と、同じランダムテープ $rV113$ による再実行を繰り返すことにより最終的に検証装置 106 が受理するような証明システムを模擬装置 110 と検証装置 106 とで再現することが可能となる。

【0105】

最終的に検証装置 106 が受理した数値列を n_1 、 n'_1 、 n_2 、 n'_2 、 \dots 、 n_k 、 n'_k としてこれを識別装置 112 への入力とする。

<二つの分布の識別不可能性>

ここで言う弱計算量的零知識証明における二つの分布が見分けがつかないとはどういうことか説明する。

【0106】

二つの分布の相違を識別する識別装置 112 は、証拠 103 と、共通入力 104、識別装置 112 の持つランダムテープ $rD117$ とが入力され、二つの分布として対話データ 107 である m_1 、 m'_1 、 m_2 、 m'_2 、 \dots 、 m_k 、 m'_k 、ランダムテープ $rV108$ の入力と、または数列 n_1 、 n'_1 、 n_2 、 n'_2 、 \dots 、 n_k 、 n'_k 、ランダムテープ $rV113$ が入力されると、証明装置 105 と検証装置 106 による分布か模擬装置 110 による分布かを判定し、結果として証明装置 105 と検証装置 106 による真の分布と判断すると 1、模擬装置 110 による分布と判断すると 0 を出力するとする。

【0107】

定められたランダムテープ $rG101$ 、 $rP109$ 、 $rV109$ 、 $rD117$ の分布から一様無作為にそれぞれのランダムテープを選んだときに、対話データ 107 と、ランダムテープ $rV108$ 、証拠 103 が入力された識別装置 112 が 1 を出力する確率を

$$Pr_{\{rG, rP, rV, rD\}} [D(m_1, \dots, m'_k, rV, W) =$$

1] と記す。

【0108】

定められたランダムテープ $rG101$ 、 $rS114$ 、 $rD117$ の分布から一様無作為にそれぞれのランダムテープを選んだときに、数列 n_1 、 n'_1 、 n_2 、 n'_2 、 \dots 、 n_k 、 n'_k 、ランダムテープ $rV113$ 、証拠 103 が入力された識別装置 112 が 1 を出力する確率を

$$Pr_{\{rG, rS, rD\}} [D(n_1, \dots, n'_k, rV, W) = 1]$$

と記す。

【0109】

この時、どのような識別装置 112 を用いても、

$$Pr_{\{rG, rP, rV, rD\}} [D(m_1, \dots, m'_k, rV, W) = 1] \text{ と } Pr_{\{rG, rS, rD\}} [D(n_1, \dots, n'_k, rV, W) = 1]$$

[零知識証明クラスと弱計算量的零知識クラスの差異]

零知識証明クラスと弱計算量的零知識証明クラスとの違いは、弱計算量的零知識証明クラスの場合には、識別装置 112 の決定する確率が、生成装置 100 のランダムテープ $rG101$ の共通入力 104 の分布に対してもとられていることと、識別装置 112 に証拠 103 が入力されることである。

【0110】

すなわち、零知識証明クラスに属することを証明する場合、「ある特定」の共通入力 104 に対する、模擬装置 110 で再現生成された模擬証明履歴 115 (数値の列) と証明装置 105 による真の証明履歴 111 である対話データ 107 とランダムテープ $rV108$ 等との分布の相違を識別することが「どのような識別装置」も不可能なクラスであった。

【0111】

しかし、弱計算量的零知識証明クラスではあらゆる共通の入力 (様々な生成装置 $G100$ のランダムテープ $rG101$ により生成された共通入力 104) が与えられたときにも「証明者の知識証拠 103 」を使っても識別できる識別装置 112 がなければ良かった。

【0112】

記号を使って書くと、零知識証明クラスではどのような識別装置 112 に対しても、全ての生成装置 100 のランダムテープ $rG101$ に対して、

$$\Pr_{_} \{rP, rV, rD\} [D(m_1, \dots, m'_k, rV) = 1] \text{ と}$$
$$\Pr_{_} \{rS, rD\} [D(n_1, \dots, n'_k, rV) = 1]$$

の差が無視できることが求められたが、

弱計算量的零知識証明クラスではどのような識別装置 112 に対しても、

$$\Pr_{_} \{rG, rP, rV, rD\} [D(m_1, \dots, m'_k, rV, W) = 1] \text{ と}$$
$$\Pr_{_} \{rG, rS, rD\} [D(n_1, \dots, n'_k, rV, W) = 1]$$

の差が無視できることが求められる。

【0113】

ここで、確率の計算に rG と W を使用するか否かに関する違いに注意されたい。

【0114】

この確率の取り方の違いを図 11 と図 12 のフローチャートを参照しながら説明する。

【0115】

生成装置 100 のランダムテープ $rG101$ に対する、

$\Pr_{_} \{rP, rV, rD\} [D(m_1, \dots, m'_k, rV) = 1]$ とは以下の図 11 の (a) のフローチャートで計算される平均値である。

【0116】

生成装置 100 のランダムテープ $rG101$ を入力して (ステップ 1101)、証明装置 105 のランダムテープ rP を決定して (ステップ 1102)、続いて検証装置 106 のランダムテープ rV を決定して (ステップ 1103)、次に識別装置 112 のランダムテープ rD を決定して (ステップ 1104)、上記決定値から証明履歴 111 を生成し (ステップ 1105)、識別結果を 1 か 0 として出力する (ステップ 1106)。

【0117】

(ステップ1113)にて全ての場合を尽くしたかをチェックし、尽くしていない場合は、(ステップ1102)まで戻り、組として異なる(r_P 、 r_V 、 r_D)を決定して再度識別結果を1か0として出す。

【0118】

これを全ての(r_P 、 r_V 、 r_D)の可能性について行い(ステップ1113)のチェックで全ての場合を尽くしたことが判定されると、識別結果の平均値を出して終了する(ステップ1112)。

【0119】

生成装置100のランダムテープ r_{G101} に対する、 $Pr_{\{r_S, r_D\}} [D(n_1, \dots, n'_k, r_V) = 1]$ とは以下の図11の(b)のフローチャートで計算される平均値である。

【0120】

生成装置100のランダムテープ r_{G101} を入力して(ステップ1107)、模擬装置110のランダムテープ r_S を決定して(ステップ1108)、続いて識別装置112のランダムテープ r_D を決定して(ステップ1109)、上記決定値から模擬証明履歴115を生成し(ステップ1110)、識別結果として1か0を出力する(ステップ1111)。この時の識別装置112は(ステップ1105)のそれと同一である。

【0121】

(ステップ1114)で全ての場合を尽くしたかをチェックし、尽くしていない場合は(ステップ1108)まで戻り、組として異なる(r_S 、 r_D)を決定して再度識別結果を1か0として出す。これを全ての(r_S 、 r_D)の可能性について行い、識別結果の平均値を出す(ステップ1115)。

$Pr_{\{r_G, r_P, r_V, r_D\}} [D(m_1, \dots, m'_k, r_V, W) = 1]$ とは以下の図12の(a)のフローチャートで計算される平均値である。

【0122】

生成装置100のランダムテープ r_G を決定して(ステップ1201)、証明装置105のランダムテープ r_P を決定して(ステップ1202)、続いて検証装置106のランダムテープ r_V を決定して(ステップ1203)、次に識別装

置 112 のランダムテープ rD を決定して（ステップ 1204）、上記決定値から証明履歴 111 と証拠 103 を生成し（ステップ 1205）、（ステップ 1205）で生成した値から識別結果を 1 か 0 として出力する（ステップ 1206）。

【0123】

（ステップ 1113）で全ての場合を尽くしたかをチェックし、尽くしていないと（ステップ 1101）まで戻り、生成装置 100 のランダムテープ rG 1201 の決定し、同様にして、組として異なる（ rG 、 rP 、 rV 、 rD ）を決定して再度識別結果として 1 または 0 を出力する。これを全ての（ rG 、 rP 、 rV 、 rD ）の可能性について行い、識別結果の平均値を出す（ステップ 1213）。

$P r _ \{rG, rS, rD\} [D(n_1, \dots, n'_k, rV, W) = 1]$ とは以下の図 12 の（b）のフローチャートで計算される平均値である。

【0124】

生成装置 100 のランダムテープ rG を決定して（ステップ 1207）、模擬装置 110 のランダムテープ rS を決定して（ステップ 1208）、次に識別装置 112 のランダムテープ rD を決定して（ステップ 1209）、上記値から模擬証明履歴 115 と証拠 103 を生成し（ステップ 1210）、（ステップ 1210）で生成した値から識別結果として 1 か 0 を出力する（ステップ 1211）。

【0125】

この時の識別装置 112 は（ステップ 1205）のそれと同一である。

【0126】

その後、（ステップ 1207）の生成装置 G のランダムテープ rG の決定まで戻り、組として異なる（ rG 、 rS 、 rD ）を決定して再度識別結果を 1 または 0 として出す。これを全ての（ rG 、 rS 、 rD ）の可能性について行い、識別結果の平均値を出す（ステップ 1215）。

【0127】

ある特定の共通入力 104 にのみ特化した、証明者さえも知らない事実を使っ

て二つの分布の相違を識別する識別装置 112 があれば、その証明システムは零知識証明クラスに属することができない。しかし、このような識別装置 112 があらゆるそのほかの大部分の共通入力 104 には有効でなかった場合、この証明システムは弱計算量的零知識証明クラスでは有り得る。このように、弱計算量的零知識証明クラスは、零知識証明クラスよりも広いクラスである。

【0128】

識別装置 112 は、証明システムが弱計算量的零知識証明クラスに属するかの評価やその評価に使用した二つの分布情報等を含む評価結果を識別装置 112 の磁気ディスク装置等に記憶する。

〔弱計算量的零知識クラスの有効性〕

もしある証明システムが、弱計算量的零知識クラスに属するならば、このプロトコルが隠したい知識を漏らさないことを保証することは次のようにして証明される。

【0129】

もし、証明システムを通じて、証明装置 105 が知っている証拠 103 あるいは証拠 103 の一部を、検証装置 106 が知り得るとする。その時、模擬装置 110 が証明装置 105 の助けを借りずに検証装置 106 の助けにより再現した模擬証明履歴 115、あるいは、真の証明履歴 111 が与えられた識別装置 112 は、その履歴が真であると仮定してこれから証明装置 105 の漏らしたであろう知識を計算する。

【0130】

識別装置 112 は元々証明装置 105 の証拠 103 を知っているのです、これと計算した証拠 103 とを比較する。もし履歴が真のものであれば、識別装置 112 は証明装置 105 の知識の引き出しに成功するはずであるから、両者は高い確率で一致するが、履歴が証明装置 105 の助けなくして検証装置 106 の助けのみで作られたものならば両者はほとんど一致しない（もし二つの履歴が一致するならば、検証装置 106 がこの知識を知らなかったという仮定に反する）。

【0131】

よって、識別装置 112 は、二つの履歴が一致するかしないかによって、履歴

の真偽を識別することができる。 よって、もし証明システムにおいて証明装置 105 が知識を漏らすならば、履歴の真偽を識別できる識別装置 112 が存在するといえる。逆に、いかなる識別装置 112 にも二つの履歴の相違を識別できないことが証明されれば、証明システムにおいて証明装置 105 は知識を漏らさないことが証明される。これは弱計算量的零知識クラスに属する証明システムであった。

【0132】

次に本発明の第2の実施の形態について説明する。

【0133】

従来の方法の零知識証明クラスに属する証明システムで、従来技術で説明したように、特別な場合において、ハッシュ関数を使用することによって、検証装置から証明装置にデータを送信する必要がなくなった。このことを弱計算量的零知識証明クラスに属する証明システムでも適用する。

【0134】

生成装置 500 と証明装置 505 と検証装置 506 とからなる $(X, W) \in R$ なる W を知っていることの証明システムで、 W に関する情報を何も漏らさないことを保証したまま、証明する方法を図5、図6を参照しながら説明する。

【0135】

これをハッシュ関数を用いた弱計算量的零知識証明クラスに属する方法と呼ぶ。

【0136】

生成装置 500 は、第1の実施の形態で説明したのと同様に、ランダムテープ $rG501$ と生成装置 500 以外によって決定される固定データ 502 が与えられたら、ランダムテープ $rG501$ を利用して、一様無作為に証拠 503 を選び、次に $(X, W) \in R$ となるような関係を持った共通入力 504 を一様無作為に生成する。

【0137】

共通入力 504 は、証明装置 505 と検証装置 506 に入力され、証拠 503 は証明装置 505 にのみ入力される。共通入力 504 を証明装置 505 と検証装

置 506 の共通の入力と呼ぶ。

【0138】

証明装置 505 は、証明部 507 と、証明部 507 から与えられたデータに対してハッシュを行うハッシュ部 508 とから構成される。

【0139】

証明部 507 とハッシュ部 508 とで互いに交換される交換データ 509 を、通信される順番に m_1 、 m'_1 、 m_2 、 m'_2 、 \dots 、 m_{k-1} 、 m'_{k-1} 、 m_k とする。

【0140】

m_1 、 \dots 、 m_k は、ハッシュ部 508 から証明部 507 へ送られるデータで、証明部 507 から送られてきたデータのハッシュ値である。

【0141】

m'_1 、 \dots 、 m'_{k-1} は、証明部 507 からハッシュ部 508 へ送られるデータとする。

【0142】

尚、証明部 507 とハッシュ部 508 の間で交換される交換データ 509 は、前述した証明装置 105 と検証装置 106 間で交換される対話データ 107 と同様な内容を有するものとする。

【0143】

交換データ 509 が生成されると、次に、 m'_1 、 \dots 、 m'_{k-1} を含む m'_k を証明装置 505 から検証装置 506 へ送る。

【0144】

また、証明装置 505 に入力される乱数を記録したランダムテープをランダムテープ $rP515$ とする。ランダムテープ $rG501$ 、 $rP515$ 、を決めると交換データ 509 m_1 、 m'_1 、 m_2 、 m'_2 、 \dots 、 m_k 、 m'_k が得られる。

【0145】

検証装置 506 は、検証部 511 とハッシュ部 512 とからなる。

【0146】

検証部 511 は、証明装置 505 から受信した m'_k から m'_1 、 \dots 、 m'_{k-1} を生成し、これをハッシュ部 512 に送る。ハッシュ部 512 はハッシュ値 m_1 、 \dots 、 m_k を生成して検証部 511 に送る。

【0147】

検証部 511 は、この結果と共通入力 504 と、 m'_k とが検証のための式を満たすかを確認することにより、OK または NG を出力する。

【0148】

ここでハッシュ部 508 から証明部 507 に送られるハッシュデータを全て乱数 609 に入れ替えた改変証明装置 605 を考える。

【0149】

この改変証明装置 605 の、一様無作為に選ばれるランダムテープ $rG501$ 、 $rP511$ 、乱数 609 に対する交換データ $618m_1$ 、 m'_1 、 m_2 、 m'_2 、 \dots 、 m_k 、 m'_k とからなる改変証明履歴 610 の分布を考える。

【0150】

この分布は証拠 503 を知っている改変証明装置 605 により生成されるものであるが、この分布と、もしランダムテープ $rS114$ の入力されるある模擬装置 612 が存在して、模擬装置 612 が改変証明装置 605 といっさい通信せずに生成する数値の列（模擬改変証明履歴 611） n_1 、 n'_1 、 n_2 、 n'_2 、 \dots 、 n_k 、 n'_k の、ランダムテープ $rG501$ 、 $rS114$ に対する分布とを、証拠 503 とランダムテープ $rD617$ が入力されたいかなる識別装置 613 にも識別できないのならば、証明装置 505 の証拠 503 を知っていることの証明はハッシュ関数を用いた弱計算量的零知識証明クラスに属していると呼ぶ事にする。

【0151】

このようなハッシュ関数を用いた弱計算量的零知識証明クラスに属する証明システムを使って知識の証明をすることが、第 2 の実施の形態の内容である。

<検証者単独でのプロトコル再現装置の構成方法>

プロトコルの模擬を行う模擬装置 612 は、改変証明装置 605 のハッシュ部 508 の出力するデータ列を全て乱数 609 に置き換える。模擬装置 612 には

証明装置 505 と検証装置 V506 の共通の入力である共通入力 504 が入力される。

【0152】

模擬装置 612 は、改変証明装置 605 から検証装置 506 へ送られるハッシュ値以外のデータ、検証部 507 からハッシュ部 508 へ送られるデータを検証装置 506 の検証に通過するよう生成する。但し検証装置 506 の検証が通過するデータとは、検証装置 506 がハッシュ部 508 から検証部 507 へ送られるデータをハッシュ関数を用いて再生成するのではなく模擬装置 612 から受け取った乱数 609 を用いた場合に検証を通過するデータのことである。

＜二つの分布の識別不可能性＞

ここで言う二つの分布が見分けがつかないとは、第 1 の実施の形態で述べた事と同じである。但し、確率は検証装置 506 のランダムテープ r_V に関して取るかわりに、乱数 609 に関して取る。

【0153】

記号を使って書くと、識別不可能とは、どのような識別装置 613 に対しても

$$\Pr_{\{r_G, r_P, \text{乱数 } 609, r_D\}} [D(m_1, \dots, m'_k, W) = 1] \text{ と}$$

$$\Pr_{\{r_G, r_S, r_D\}} [D(n_1, \dots, n'_k, W) = 1]$$

の差が無視できることである。

【0154】

零知識証明の場合では、全ての生成装置 500 のランダムテープ r_G 501 に対して、

$$\Pr_{\{r_P, \text{乱数 } 609, r_D\}} [D(m_1, \dots, m'_k) = 1] \text{ と}$$

$$\Pr_{\{r_S, r_D\}} [D(n_1, \dots, n'_k) = 1]$$

の差が無視できることを要求する。

【0155】

この条件より本発明の課す条件の方が緩い。

【0156】

識別装置 6 1 3 は、評価した対象の証明システムが弱計算量的零知識証明クラスに属するかの評価やその評価に使用した二つの分布情報等を含む評価結果を磁気ディスク装置等に記憶する。

【0 1 5 7】

次に本発明の第 3 の実施の形態について説明する。

【0 1 5 8】

模擬装置と識別装置を使用する評価者により特定の証明システムが弱計算量的零知識証明クラスに属するとの評価またはその評価の根拠の情報を、提示者が被提示者に提供する方法について、図 1 0 を参照しながら説明する。

【0 1 5 9】

評価者は、パソコン等のコンピュータからなる評価者端末 1 0 0 1 によって、インターネット網や電話回線を含むネットワーク 1 0 0 4 を介して接続された一つあるいは複数の証明システムが、弱計算量的零知識証明クラスまたはハッシュ関数を用いた弱計算量的零知識証明クラスに属する証明システムであるか否かの評価結果を識別装置 1 1 2, 6 1 3 から取り出し、その内容を評価者端末 1 0 0 1 の記憶装置 1 0 0 2 に保存する。

【0 1 6 0】

提示者はパソコン等の提示者端末 1 0 0 3 からネットワーク 1 0 0 4 を介して評価者端末 1 0 0 1 から一つまたは複数の証明システムが、弱計算量的零知識証明クラスまたはハッシュ関数を用いた弱計算量的零知識証明クラスに属する証明システムであるかの評価結果または、その評価の根拠を評価者端末 1 0 0 1 の記憶装置 1 0 0 2 から取り寄せ、提示者端末 1 0 0 3 の記憶装置 1 0 0 5 に蓄える。

【0 1 6 1】

提示者は、提示者端末 1 0 0 3 によって、特定の証明システムが安全であるか否か等の評価結果または、その評価の根拠 1 0 0 9 をプリンタ装置やディスプレイ等の表示装置に出力する。

【0 1 6 2】

あるいは、提示者端末 1 0 0 3 は特定の証明システムが、安全であることをそ

の提示を要求する被提示者端末 1007 に示すため、提示者の必要に応じて被提示者端末 1007 に取り寄せた内容を送信して提示する。

【0163】

あるいは、提示者端末 1003 は被提示者端末 1007 に評価者を直接紹介して評価内容を伝える。

【0164】

あるいは、提示者は不特定多数の被提示者端末 1007 に対して前述の評価結果または、その評価の根拠をネットワーク 1004 を介して送信し提示する。

【0165】

次に本発明の第 1 の実施例について説明する。

[プロトコルの記述]

最初に、余計な知識を漏らさないことが保証された証明システムを、図 2 を参照しながら説明する。

【0166】

記号の前提として、 p 、 q を大きな素数とし、 q は $p-1$ を割りきるとする。 1 から $p-1$ までの整数を $(\mathbb{Z}/p\mathbb{Z})^*$ とする。

【0167】

$(\mathbb{Z}/p\mathbb{Z})^*$ の要素で q 乗して $\text{mod } p$ をとると 1 になるものの全体の集合を G_q とする。

【0168】

0 から $q-1$ までの要素を $\mathbb{Z}/q\mathbb{Z}$ とする。 p 、 q を領域変数 200 と呼ぶ。

【0169】

領域変数 200 p 、 q は第 1 の実施の形態で言う固定データと同じである。

【0170】

ランダムテープ $rG201$ が入力された生成装置 202 は、ランダムテープ $rG201$ を利用して G_q の要素 g 、 h 、 z' 、 $\mathbb{Z}/q\mathbb{Z}$ の要素 x を一様無作為に生成し、 $y = g^x \text{ mod } p$ とする。

【0171】

この時、 G_q の元 z' は圧倒的な確率で不等式 $z' \neq h^x \pmod{p}$ となる。

【0 1 7 2】

対話証明装置 2 0 3 には共通入力 2 0 4 p 、 q 、 g 、 h 、 y 、 z' 及び、証拠 2 0 5 及びランダムテープ $r P$ 2 0 6 が入力される。

【0 1 7 3】

対話検証装置 2 0 7 には共通入力 2 0 4 p 、 q 、 g 、 h 、 y 、 z' 及びランダムテープ $r V$ 2 0 8 が入力される。

【0 1 7 4】

対話検証装置 2 0 7 は、対話検証装置 2 0 7 の持っている情報のみから不等式 $z' \neq h^x \pmod{p}$ が成り立つことを知ることは現実的には不可能である。

【0 1 7 5】

対話証明装置 2 0 3 は、対話検証装置 2 0 7 に、不等式 $z' \neq h^x \pmod{p}$ が成り立つことを以下の手順で証明する。これは (g, h, y, z') が、ディフィーヘルマン事例でないことの証明である。

(1) 対話検証装置 2 0 7 は、ランダムテープ $r V$ 2 0 8 を利用して Z/qZ の要素である乱数 2 1 2 とチャレンジ 2 1 1 を一様無作為に選び、チャレンジコミットメント 2 0 9 の $a = g^b y^c \pmod{p}$ を生成し、対話証明装置 2 0 3 に生成したチャレンジコミットメント 2 0 9 を送る。

(2) 対話証明装置 2 0 3 は、ランダムテープ $r P$ 2 0 6 を利用して Z/qZ の要素 d 、 e 、 f を一様無作為に選び、

$$h' = h^d \pmod{p},$$

$$w' = z'^d \pmod{p},$$

$$v = h^{x^d} \pmod{p} \text{ を計算する。さらに、}$$

$$y' = g^e \pmod{p},$$

$$v' = h'^e \pmod{p},$$

$$h'' = h^f \pmod{p},$$

$w'' = z' f \pmod{p}$ を計算し、

対話検証装置 207 に計算値 $214 h'$ 、 w' 、 v 、 y' 、 v' 、 h'' 、 w'' を送る。

(3) 対話検証装置 207 は、乱数 212、チャレンジ 211 を対話証明装置 203 に送る。

(4) 対話証明装置 203 は、

等式 $a = g^b y^c \pmod{p}$ が成り立つことを確認する。

この式が成り立たなかった場合は、プロトコルを中止する。

(5) 対話証明装置 203 は、(2) にて生成した d 、 e 、 f 213 及び証拠 205 を用いて、レスポンス 218 の r 、 r' を

$$r = xc + e \pmod{q},$$

$$r' = dc + f \pmod{q}$$

として対話検証装置 207 に送る。

(6) 対話検証装置 207 は対話証明装置 203 から受け取った計算値 $214 h'$ 、 w' 、 v 、 y' 、 v' 、 h'' 、 w'' と、レスポンス 218 r 、 r' と、チャレンジ 211 と、共通入力 204 p 、 q 、 g 、 h 、 y 、 z' と、を用いて

$$g^r = y^c y' \pmod{p},$$

$$h'^r = v^c v' \pmod{p},$$

$$h^{r'} = h'^c h'' \pmod{p},$$

$$z'^{r'} = w'^c w'' \pmod{p},$$

$$v \neq w' \pmod{p} \text{ が成り立てば、}$$

$$y = g^x \pmod{p} \text{ である } x \text{ に対して}$$

不等式 $z' \neq h^x \pmod{p}$ であることを受理し OK を出力する。

でなければ NG を出力する。

【0176】

対話検証装置 207 の検証者がこのプロトコルから知り得たデータは、対話検証装置 207 の検証者が対話証明装置 203 の証明者と無関係に保持しているデータを含めて、対話検証装置 207 のランダムテープ rV 、 p 、 q 、 g 、 h 、 y 、 z' 、 a 、 b 、 c 、 h' 、 w' 、 v 、 y' 、 v' 、 h'' 、 w'' 、 r 、 r'

である。これは図1の証明履歴111に相当するものである。

[弱計算量的零知識の証明方法]

<模擬装置が証明装置を使わず検証装置だけ使ってプロトコルを再現する方法>

証明システムの模擬を行う模擬装置が、検証装置を用いて、証明装置と通信することなく模擬された証明履歴 rV 、 p 、 q 、 g 、 h 、 y 、 z' 、 a 、 b 、 c 、 h' 、 w' 、 v 、 y' 、 v' 、 h'' 、 w'' 、 r 、 r' (図1の模擬証明履歴115) を生成する方法について図3を参照しながら説明する。

(1) 模擬装置300には生成装置202の出力した領域変数 p 、 q 、とランダムテープ $rG201$ のデータ g 、 h 、 y 、 z' 204 及び模擬装置300のランダムテープ $rS301$ が入力される。

(2) 検証装置207には p 、 q 、 g 、 h 、 y 、 z' が入力される。

(3) 模擬装置300はランダムテープ $rS301$ を利用して検証装置207の入力となるランダムテープ $rV302$ を生成する。

(4) 模擬装置300は、検証装置207に、ランダムテープ $rV302$ を入力すると、検証装置207は、乱数212とチャレンジ211を選択し、チャレンジコミットメント209 $a = g^b y^c \pmod{p}$ を計算して a を出力する。

(5) 模擬装置300は、ランダムテープ $rS301$ を利用して一様無作為に選んだ G_q の要素 h' 、 w' 、 v 、 y' 、 v' 、 h'' 、 w'' を検証装置207に入力する。

【0177】

すると検証装置207は、乱数212、チャレンジ211を出力する。模擬装置300は、チャレンジコミットメント209を用いて、 $a = g^b y^c \pmod{p}$ を確認する。成り立たなければシステムを中断する。

(6) 模擬装置300は、検証装置207をリセットする。そして再度同じランダムテープ $rV302$ を入力する。すると、検証装置207は、同じチャレンジコミットメント209を再度出力する。

(7) 模擬装置300はランダムテープ $rS301$ を利用して一様無作為に G_q の要素から w' を、 Z/qZ の要素から i 及び r 、 r' 308を選ぶ。また

、(5)で獲得したチャレンジ211を用いて、コミットメント

$$h' = g^i \bmod p$$

$$v = y^i \bmod p$$

$$y' = g^r y^{-c} \bmod p、$$

$$v' = h'^r v^{-c} \bmod p、$$

$$h'' = h'^r h'^{-c} \bmod p、$$

$$w'' = z'^r w'^{-c} \bmod p、$$

を計算し、 w' と共に検証装置207に入力する。

(8) 検証装置207は最初に出力したものと同一乱数212、チャレンジ211を出力する。

(9) 模擬装置300は、 r 、 r' を検証装置207に送る。

(10) 検証装置207は、証明の受理21を出力する。

<検証者が単独で生成した値の列と、証明者と共同で生成した値の列の違い>

証明装置を使用する証明者が関わる真のプロトコルでは、 w' は $\log_h z' = \log_{h'} w'$ となるように選ばれる。証明装置の代わりに模擬装置を使用する検証者が単独で再現したプロトコルでは w' は一様無作為に選ばれ、このような等式は成立しない。その他の値の差異は全てこの違いにより生ずる。

【0178】

あるアルゴリズムが存在して、これに i 及び片方の値の列が入力されたときに、もし一様無作為に選ばれた x に対して、高い確率で両者の違いを判別することできるならば、このアルゴリズムを使ってディフィーヘルマン判別問題を解くことができる。ディフィーヘルマン判別問題とは4個の数値 a 、 b 、 c 、 d が与えられたときに $\log_a b = \log_c d$ かを判別する問題である。この問題は a 、 b 、 c 、 d が十分に大きな時は解くことは不可能とされている。本例では $\log_h z' = \log_{h'} w'$ かを判別しなければならない。

<模擬された証明履歴と、真の証明履歴を識別できないことの証明>

模擬装置が証明装置を利用することなく、検証装置のみを利用して生成した証明履歴と、証明装置が検証装置と共同で生成した真の証明履歴を計算量的に識別できないことの証明を図4を参照しながら説明する。

【0179】

ディフィーヘルマン事例生成装置 G_{DH400} を次のように構成する。

【0180】

ディフィーヘルマン事例生成装置 G_{DH400} にはランダムテープ r_{GDH401} と領域変数 $200p$ 、 q が入力される。ディフィーヘルマン事例生成装置 G_{DH400} はランダムテープ r_{GDH401} を利用して G_q の元 α 、 β と、 Z/qZ の元 θ を一様無作為に生成する。

【0181】

G_q の元 $\gamma = \alpha^\theta \pmod{p}$ 、 $\delta = \beta^\theta \pmod{p}$ を生成する。最後に、事例 402α 、 β 、 γ 、 δ を出力する。

【0182】

ランダム事例生成装置 G_R403 を次のように構成する。

【0183】

ランダム事例生成装置 G_R403 にはランダムテープ r_{GR} と領域変数 $200p$ 、 q が入力される。ランダム事例生成装置 G_R403 は、ランダムテープ r_{GR} を利用して G_q の元の事例 402α 、 β 、 γ 、 δ を一様無作為に生成し、これらを出力する。

【0184】

ディフィーヘルマン判別問題とは、ディフィーヘルマン事例生成装置 G_{DH400} の出力である事例 402α 、 β 、 γ 、 δ あるいは、ランダム事例生成装置 G_R403 の出力である事例 α 、 β 、 γ 、 δ のどちらかが一様無作為に選ばれて与えられたときに、事例 402α 、 β 、 γ 、 δ がどちらの生成装置の出力であるかを判別問題生成装置 G_{PR406} によって判定する問題である。これを $1/2$ より有意に高い確率で判定することは計算量理論的に難しいとされている。

【0185】

今、 G_q の元の列である事例 402α 、 β 、 γ 、 δ 及びランダムテープ r_{GPR405} が入力されたとき、判別問題生成装置 G_{PR406} は、検証装置 207 を利用して以下のように証明履歴 p 、 q 、 g 、 h 、 y 、 z' 、 a 、 b 、 c 、 h' 、 w' 、 v 、 y' 、 v' 、 h'' 、 w'' 、 r 、 r' 407 を生成する。

(1) 判別問題生成装置 GPR406 は、ランダムテープ r_{GPR405} を利用して G_q の元 g 、 Z/qZ の元 x を一様無作為に生成する。

(2) 判別問題生成装置 GPR406 は、 $h = \alpha$ 、 $z' = \beta$ 、 $y = g^x \bmod p$ として、共通入力 p 、 q 、 g 、 y 、 h 、 z' 409 を検証装置 207 に入力する。

(3) 判別問題生成装置 GPR406 は、 r_{GPR405} を利用して検証装置 207 のランダムテープ r_{V410} を生成する。

(4) 判別問題生成装置 GPR406 がランダムテープ r_{V410} を検証装置 207 に入力すると、検証装置 207 はチャレンジコミットメント 209 を出力する。

(5) 判別問題生成装置 GPR406 は、 G_q の元 h' 、 w' 、 v 、 y' 、 v' 、 h'' 、 w'' 411 を一様無作為に選んで検証装置 207 に入力すると、検証装置 207 は乱数 212、チャレンジ 211 を判別問題生成装置 GPR406 に出力する。

(6) 判別問題生成装置 GPR406 は、検証装置 207 をリセットし、(2) と同じ p 、 q 、 g 、 y 、 h 、 z' 409 及び (4) と同じランダムテープ r_{V408} を検証装置 207 に入力すると、検証装置 207 は同じチャレンジコミットメント 209 を出力する。

(7) 判別問題生成装置 GPR406 は、一様無作為に Z/qZ の要素から、リスpons 413 を選ぶ。(5) で受け取った c を利用して、

$$h' = \gamma、$$

$$w' = \delta、$$

$$v = h'^x \bmod p、$$

$$y' = g^{ry-c} \bmod p、$$

$$v' = h'^{rv-c} \bmod p、$$

$$h'' = h^{r'h'-c} \bmod p、$$

$$w'' = z'^{r'w'-c} \bmod p、$$

$$a = g^{byc} \bmod p、$$
 を生成する。

【0186】

判別問題生成装置 GPR406 は、最後に証明履歴

$p, q, g, h, y, z', a, b, c, h', w', v, y', v', h', w', r, r'$ 407 及び証拠 417 を出力する。

【0187】

検証装置 207 の検証手段 220 は動かさなくて良い。

【0188】

もし、判別問題生成装置 GPR406 に入力された事例 402 $\alpha, \beta, \gamma, \delta$ が、ディフィーヘルマン事例生成装置 GDH400 より出力されたものならば、ランダムテープ $rGDH401, rGPR405$ をランダムに選んだときの、判別問題生成装置 GPR406 の出力する証明履歴及び証拠 407、 $p, q, g, h, y, z', a, b, c, h', w', v, y', v', h', w', r, r', x$ の分布は、真の証明装置と検証装置が互いに通信することによって得られる、ランダムテープ $rG201, rP206, rV208$ をランダムに選んだときの、証明履歴 $p, q, g, h, y, z', a, b, c, h', w', v, y', v', h', w', r, r'$ 及び $x205$ の分布と同一になる。

【0189】

もし、判別問題生成装置 GPR406 に入力された事例 402 $\alpha, \beta, \gamma, \delta$ が、ランダム事例生成装置 GR403 より出力されたものならば、ランダムテープ $rGR404, rGPR405$ をランダムに選んだときの、判別問題生成装置 GPR406 の出力する証明履歴及び証拠 407、 $p, q, g, h, y, z', a, b, c, h', w', v, y', v', h', w', r, r', x$ の分布は、模擬装置 300 と検証装置 207 が互いに通信することによって得られる、 $rG201, rS301$ をランダムに選んだときの、模擬された証明履歴 $p, q, g, h, y, z', a, b, c, h', w', v, y', v', h', w', r, r'$ 及び生成装置 202 の出力する証拠 205 の分布と同一になる。

【0190】

以上より、仮に真の証明装置 P203 と検証装置 207 が互いに通信することによって得られる、証明履歴 $p, q, g, h, y, z', a, b, c, h', w', v, y', v', h', w', r, r'$ と、模擬装置 300 と検証装置

207が互いに通信することによって得られる、模擬された証明履歴 p 、 q 、 g 、 h 、 y 、 z' 、 a 、 b 、 c 、 h' 、 w' 、 v 、 y' 、 v' 、 h'' 、 w'' 、 r 、 r' を識別することができる、証拠 205が入力された識別装置 112が存在するとする。

【0191】

ならば、ディフィーヘルマン事例生成装置 $G_{DH}400$ またはランダム事例生成装置 G_R403 のどちらの出力であるか分からない事例 402α 、 β 、 γ 、 δ の組が与えられたとき、これを判別問題生成装置 $G_{PR}406$ に入力して、証明履歴及び証拠 $407p$ 、 q 、 g 、 h 、 y 、 z' 、 a 、 b 、 c 、 h' 、 w' 、 v 、 y' 、 v' 、 h'' 、 w'' 、 r 、 r' 、 x を出力させ、これを識別装置 112に入力し、この値の列が真の列か模擬の列かを判別させることにより、事例 402α 、 β 、 γ 、 δ の組がディフィーヘルマン事例生成装置 $G_{DH}400$ またはランダム事例生成装置 G_R403 のどちらの出力かを判定することができる。これはディフィーヘルマン判別問題が難しいことと矛盾する。よって、上記のような識別装置 112は存在しない。

【0192】

上記理由より、二つの数値の列を識別することは不可能なため、本実施例の証明プロトコルは弱計算量的零知識クラスに属することが証明される。

<零知識証明に属さないことの証明>

本実施例が零知識証明に属さないことを図 13を参照しながら証明する。

【0193】

識別装置' 1301として、特別な場合に有効な値 1302としてある Z/q の数 x' を準備し、模擬された証明履歴 1304または真の証明履歴 1305である p 、 q 、 g 、 h 、 y 、 z' 、 a 、 b 、 c 、 h' 、 w' 、 v 、 y' 、 v' 、 h'' 、 w'' 、 r 、 r' 、 x 1303が入力されたとき、
等式 $z' = h^{x'} \pmod{p}$ かつ $w' = h' x' \pmod{p}$ であれば、

真の証明システムの出力した履歴であると判断し、

等式 $z' = h^{x'} \pmod{p}$ かつ不等式 $w' \neq h' x' \pmod{p}$

であれば、模擬された履歴であると判断するとする。この識別装置は生成装置 202 が、

等式 $x' = \log_h z'$ なる g 、 y 、 h 、 z' を生成した場合には、全てのランダムテープ r_{p1306} 、 r_{v1307} 、 r_{s1308} 、識別装置のランダムテープ 1310 の場合に対して正しく真／模擬の識別を行うことができる。

【0194】

ここで、生成装置のランダムテープが特別なものに関してのみ識別でき、その他の場合には識別ができないことに注意する。このように、生成装置のたった一つ出力に対しても正しく識別できる識別装置が存在するものは零知識証明ではない。ただし、大多数の $\log_h z'$ の場合に関して正しく真／模擬を判別する識別装置は存在しないので、弱計算量的零知識証明である。

【0195】

次に第 2 の実施例について説明する。

[プロトコルの記述]

最初に、証明において検証装置から証明装置へのデータの送信が不要なプロトコルで、余計な知識を漏らさないことが保証された証明システムを、図 7 を参照しながら説明する。

【0196】

p 、 q をそれぞれ大きな素数で q は $p-1$ を割りきるとする。1 から $p-1$ までの整数を $(Z/pZ)^*$ とする。

【0197】

$(Z/pZ)^*$ の要素で q 乗して $\text{mod } p$ をとると 1 になるもの全体の集合を G_q とする。0 から $q-1$ までの要素を Z/qZ とする。 p 、 q を領域変数 700 と呼ぶ。

【0198】

ランダムテープ r_{G701} が入力された生成装置 702 は、ランダムテープ r_{G701} 利用して G_q の要素 g 、 h 、 z' と Z/qZ の要素 x を一様無作為に生成し、 $y = g^x \text{ mod } p$ とする。この時 G_q の元 z' は圧倒的な確率で不等式 $z' \neq h^x \text{ (mod } p)$ が成り立つ。

【0199】

証明装置 703 には共通入力 p 、 q 、 g 、 h 、 y 、 z' 704 及び証拠 705 及びランダムテープ r_P 706 が入力される。

【0200】

検証装置 707 には共通入力 p 、 q 、 g 、 h 、 y 、 z' 704 が入力される。
検証装置 707 は検証装置 707 の持っている情報から
不等式 $z' \neq h^x \pmod{p}$ であることを知ることは現実的には不可能である。

【0201】

証明装置 703 は検証装置 707 に不等式 $z' \neq h^x \pmod{p}$ であることを以下の手順で証明する。これは (g, h, y, z') ディフィーヘルマン事例でないことの証明である。

(1) 証明装置 703 はランダムテープ r_P 706 を利用して Z/qZ の要素 d 、 e 、 f を一様無作為に選び、コミットメント

$$h' = h^d \pmod{p},$$

$$w' = z'^d \pmod{p},$$

$$v = h^{xd} \pmod{p},$$

$$y' = g^e \pmod{p},$$

$$v' = h'^e \pmod{p},$$

$$h'' = h^f \pmod{p},$$

$$w'' = z'^f \pmod{p} \text{ を計算する。}$$

(2) 証明装置 703 はハッシュ関数 $\text{Hash}()$ を用いてチャレンジ 711
 $c = \text{Hash}(p, q, g, h, y, z', h', w', v, y', v', h'', w'')$ を生成する。

(3) 証明装置 703 は、レスポンス

$$r = xc + e \pmod{q},$$

$$r' = dc + f \pmod{q}$$

を生成する。

(4) 証明装置 703 は、 h' 、 w' 、 v 、 y' 、 v' 、 h'' 、 w'' 709

、 r 、 r' 713を検証装置707に送信する。

(5) 検証装置707は

$c' = \text{Hash}(p, q, g, h, y, z', h', w', v, y', v', h'', w'')$ を生成する。これはチャレンジ711と同じ値になる。

検証装置707は4個の等式

$$g^r = y^{c'} y' \pmod{p},$$

$$h'^r = v^{c'} v' \pmod{p},$$

$$h^{r'} = h'^{c'} h'' \pmod{p},$$

$$z'^{r'} = w'^{c'} w'' \pmod{p} \text{ と}$$

1個の不等式 $v \neq w' \pmod{p}$ が成り立てば、等式 $y = g^x \pmod{p}$ である x に対して

不等式 $z' \neq h^x \pmod{p}$ であることの受理としてOKを出力する。でなければNGを出力する。

【0202】

検証装置707がこのプロトコルから知り得たデータは、検証装置707が証明装置703と無関係に保持しているデータを含めて、 p 、 q 、 g 、 h 、 y 、 z' 、 h' 、 w' 、 v 、 y' 、 v' 、 h'' 、 w'' 、 c 、 r 、 r' である。(但し c はその他の値から計算できる。)

[弱計算量的零知識の証明方法]

<模擬装置が証明装置を使わず検証装置だけ使ってプロトコルを再現する方法>

模擬装置800が証明装置と通信することなく、 c をハッシュ値でなく乱数に置き換えた p 、 q 、 g 、 h 、 y 、 z' 、 h' 、 w' 、 v 、 y' 、 v' 、 h'' 、 w'' 、 c 、 r 、 r' を生成する方法を、図8を参照しながら説明する。

(1) 模擬装置800には領域変数700 p 、 q 及び生成装置702の生成した g 、 h 、 y 、 z' 及びである共通入力 p 、 q 、 g 、 h 、 y 、 z' 704 ランダムテープ $rS801$ が入力される。

(2) 模擬装置800はランダムテープ $rS801$ を利用して、一様無作為に G_q の要素から w' を、 Z/qZ の要素から i 、チャレンジ802、リスポンス803を選ぶ。

さらに、コミットメント

$$h' = g^i \bmod p$$

$$v = y^i \bmod p$$

$$y' = g^r y^c \bmod p、$$

$$v' = h'^r v^c \bmod p、$$

$$h'' = h'^r h'^c \bmod p、$$

$$w'' = z'^r w'^c \bmod p、$$

を計算する。

【0203】

共通入力 p, q, g, h, y, z' は始めからあるので、これと合わせて模擬された証明履歴 $808 p, q, g, h, y, z', h', w', v, y', v', h'', w'', c, r, r'$ として出力する。

<検証者が単独で生成した値の列と、証明者と共同で生成した値の列の違い>

証明者が関わる真のプロトコルとでは、 w' は $\log_h z' = \log_h w'$ となるように選ばれるが、検証者が単独で再現したプロトコルでは w' は一様無作為に選ばれ、このような等式は成立しない。その他の値の差異は全てこの違いにより生ずる。

【0204】

あるアルゴリズムが存在して、これに i 及び片方の値の列が入力されたときに、もし一様無作為に選ばれた x に対して、高い確率で両者の違いを判別することができるならば、このアルゴリズムを使ってディフィーヘルマン判別問題を解くことができる。

【0205】

ディフィーヘルマン判別問題とは4個の数値 a, b, c, d が与えられたときに $\log_a b = \log_c d$ かを判別する問題である。この問題は a, b, c, d が十分に大きな時は解くことは不可能とされている。本例では $\log_h z' = \log_h w'$ かを判別しなければならない。

<検証者が単独で生成した値の列と、証明者と共同で生成した値の列を判別できないことの証明>

模擬装置が証明装置を利用することなく生成した証明履歴と、証明者が生成した真の証明履歴を計算量的に識別できないことの証明を図9を参照しながら説明する。

【0206】

ディフィーヘルマン事例生成装置 G_{DH900} 、ランダム事例生成装置 G_{R901} 、ランダムテープ r_{GDR902} 、 r_{GR903} 、 α 、 β 、 γ 、 δ_{904} の定義は実施例1と同じである

G_q の元の列 α 、 β 、 γ 、 δ_{904} 及びランダムテープ r_{GPR905} が入力されたとき、判別問題生成装置 G_{PR906} は以下のように証明履歴 $907p$ 、 q 、 g 、 h 、 y 、 z' 、 h' 、 w' 、 v 、 y' 、 v' 、 h'' 、 w'' 、 c 、 r 、 r' と証拠 908 を生成する。

(1) 判別問題生成装置 G_{PR906} は、ランダムテープ r_{GPR} を利用して G_q の元 g 、 Z/qZ の元である証拠 908 、チャレンジ 910 、レスポンス 911 を一様無作為に生成する。

(2) 判別問題生成装置 G_{PR906} は、 $h = \alpha$ 、 $z' = \beta$ 、 $y = g^x \bmod p$ 、と計算して、共通入力を p 、 q 、 g 、 h 、 y 、 z' 、証拠を x とする。

(3) 判別問題生成装置 G_{PR906} は、コミットメント

$$h' = \gamma、$$

$$w' = \delta、$$

$$v = h'^x \bmod p、$$

$$y' = g^{ry-c} \bmod p、$$

$$v' = h'^{rv-c} \bmod p、$$

$$h'' = h^{r'h'-c} \bmod p、$$

$$w'' = z'^{r'w'-c} \bmod p、$$

を生成する。

【0207】

最後に証明履歴 $907p$ 、 q 、 g 、 h 、 y 、 z' 、 h' 、 w' 、 v 、 y' 、 v' 、 h'' 、 w'' 、 c 、 r 、 r' 及び証拠 908 を出力する。

【0208】

もし GPR906 に入力された α 、 β 、 γ 、 δ 904 が、ディフィーヘルマン事例生成装置 GDH900 より出力されたものならば、ランダムテープ rGDH902、rGPR905、 c を決定する乱数をランダムに選んだときの、判別問題生成装置 GPR906 の出力する証明履歴 907p、 q 、 g 、 h 、 y 、 z' 、 h' 、 w' 、 v 、 y' 、 v' 、 h'' 、 w'' 、 c 、 r 、 r' 及び x の分布は、真の証明装置 703 の出力において、チャレンジ 711 を乱数に置き換えて得られる、ランダムテープ rG、rP 及び c を決定する乱数をランダムに選んだときの、証明履歴 p 、 q 、 g 、 h 、 y 、 z' 、 h' 、 w' 、 v 、 y' 、 v' 、 h'' 、 w'' 、 c 、 r 、 r' 704、709、711、713 及び証拠 705 の分布と同一になる。

【0209】

もし判別問題生成装置 GPR906 に入力された α 、 β 、 γ 、 δ 904 が、ランダム事例生成装置 GR901 より出力されたものならば、rGR903、rGPR905、及びチャレンジ 910 を決定する乱数をランダムに選んだときの、判別問題生成装置 GPR906 の出力する証明履歴 907p、 q 、 g 、 h 、 y 、 z' 、 h' 、 w' 、 v 、 y' 、 v' 、 h'' 、 w'' 、 c 、 r 、 r' 及び証拠 908 の分布は、模擬装置 800 によって得られる、rG701、rS801 をランダムに選んだときの、証明履歴 808p、 q 、 g 、 h 、 y 、 z' 、 h' 、 w' 、 v 、 y' 、 v' 、 h'' 、 w'' 、 c 、 r 、 r' 及び生成装置 702 の出力する証拠 705 の分布と同一になる。

【0210】

以上より、仮に真の証明装置 703 の出力においてチャレンジ 711 を乱数に置き換えて得られる証明履歴 p 、 q 、 g 、 h 、 y 、 z' 、 h' 、 w' 、 v 、 y' 、 v' 、 h'' 、 w'' 、 c 、 r 、 r' と、模擬装置 800 によって得られる、証明履歴 p 、 q 、 g 、 h 、 y 、 z' 、 h' 、 w' 、 v 、 y' 、 v' 、 h'' 、 w'' 、 c 、 r 、 r' を識別することができる、証拠 705 が入力された識別装置 613 が存在するとするならば、ディフィーヘルマン事例生成装置 GDH900 またはランダム事例生成装置 GR901 のどちらの出力であるか分からない α 、 β 、 γ 、 δ 904 の組が与えられたとき、これを判別問題生成装置 GPR906

に入力して、証明履歴 907 p 、 q 、 g 、 h 、 y 、 z' 、 h' 、 w' 、 v 、 y' 、 v' 、 h'' 、 w'' 、 c 、 r 、 r' 及び証拠 908 を出力させ、これを識別装置 613 に入力し、この値の列が真の列か模擬の列かを判別させることにより、 α 、 β 、 γ 、 δ 904 の組がディフィーヘルマン事例生成装置 GDH 900 またはランダム事例生成装置 GR 901 のどちらの出力かを判定することができる。これはディフィーヘルマン判別問題が難しいことと矛盾する。

【0211】

よって、上記のような識別装置 613 は存在しない。

【0212】

上記理由より、二つの数値の列を識別することは不可能なため、本実施例の証明プロトコルはハッシュ関数を用いた弱計算量的零知識クラスに属することが証明される。

【0213】

本実施例が零知識証明に属さないことを証明する。

【0214】

識別装置' として、ある Z/qZ の数 x' を準備し、証明履歴 p 、 q 、 g 、 h 、 y 、 z' 、 h' 、 w' 、 v 、 y' 、 v' 、 h'' 、 w'' 、 c 、 r 、 r' 、 x が入力されたとき、

等式 $z' = h^{x'} \pmod{p}$ かつ等式 $w' = h'^{x'} \pmod{p}$ が成り立てば真の証明システムの出力した履歴であると判断し、

等式 $z' = h^{x'} \pmod{p}$ かつ不等式 $w' \neq h'^{x'} \pmod{p}$ が成り立てば模擬された履歴であると判断するとする。

【0215】

この識別装置は、生成装置が

等式 $x' = \log_h z'$ が成り立たないような g 、 y 、 h 、 z' を生成した場合には、全てのランダムテープ r_p 、 r_v の場合に対して正しく真／模擬の識別を行うことができる。このように、生成装置のたった一つ出力に対しても正しく識別できる識別装置が存在するものは零知識証明ではない。ただし、大多数の $\log_h z'$ の場合に関して正しく真／模擬を識別装置は存在しないので、弱計算量

的零知識証明である。

【0 2 1 6】

【発明の効果】

従来の技術では、証明者が検証者に知識を漏らさないことを保証された安全な証明システムを使いたいならば、零知識証明クラスに属する証明システムを使う必要があった。しかし、本発明の弱計算量的零知識証明クラスに属する証明方法を使えば、零知識証明クラスに属さないプロトコルでも、証明者が検証者に知識を漏らさないことを保証して証明できる効果がある。

【0 2 1 7】

特に実施例 1 及び 2 のプロトコルでは、ディフィーヘルマン事例でないことを証明する方法であり、かつディフィーヘルマン事例でないことの証拠が漏れないことが保証される方法であったが、従来の零知識証明に属する方法より効率的であるという特徴を備えている。

【図面の簡単な説明】

【図 1】

本発明実施の形態 1 の生成装置、証明装置、検証装置、模擬装置、模擬装置と通信する検証装置、識別装置の関係を示したブロック図である。

【図 2】

本発明実施例 1 の生成装置、証明装置、検証装置の関係を示したブロック図である。

【図 3】

本発明実施例 1 の生成装置、模擬装置、検証装置の関係を示したブロック図である。

【図 4】

本発明実施例 1 の二つの事例生成装置、判別問題生成装置、検証装置の関係を示したブロック図である。

【図 5】

本発明実施例 2 の生成装置、証明装置、検証装置の関係を示したブロック図である。

【図 6】

本発明実施例 2 の生成装置、改変した証明装置、模擬装置、識別装置の関係を示したブロック図である。

【図 7】

本発明実施例 2 の生成装置、証明装置、検証装置の関係を示したブロック図である。

【図 8】

本発明実施例 2 の生成装置、模擬装置の関係を示したブロック図である。

【図 9】

本発明実施例 2 の二つの事例生成装置、判別問題生成装置の関係を示したブロック図である。

【図 1 0】

本発明実施の形態 3 の評価者、提示者、被提示者の関係を示したブロック図である。

【図 1 1】

本発明実施の形態 1 の解説で、零知識証明における確率の評価方法を示したフローチャートである。

【図 1 2】

本発明実施の形態 1 の解説で、本発明である弱零知識証明における確率の評価方法を示したフローチャートである。

【図 1 3】

本発明実施例 1 のプロトコルが零知識証明でないことの証明を示したブロック

【符号の説明】

- 1 0 0 生成装置
- 1 0 1 ランダムテーブル r G
- 1 0 2 固定データ
- 1 0 3 証拠
- 1 0 4 共通入力
- 1 0 5 証明装置

1 0 6	検証装置
1 0 7	対話データ
1 0 8	ランダムテープ r V
1 1 0	模擬装置
1 1 1	証明履歴
1 1 2	識別装置
1 1 3	ランダムテープ r V
1 1 5	模擬証明履歴
1 1 7	ランダムテープ r D
2 0 0	領域変数
2 0 2	生成装置
2 0 1	ランダムテープ r G
2 0 2	生成装置
2 0 3	対話証明装置
2 0 4	共通入力
2 0 5	証拠
2 0 6	ランダムテープ r P
2 0 7	対話検証装置
2 0 8	ランダムテープ r V
2 0 9	チャレンジコミットメント
2 1 1	チャレンジ
2 1 2	乱数
2 1 4	計算値
2 1 8	リスポンス
3 0 0	模擬装置
3 0 1	ランダムテープ r S
3 0 2	ランダムテープ r V
4 0 0	ディフィーヘルマン事例生成装置 G D H
4 0 1	ランダムテープ r G D H

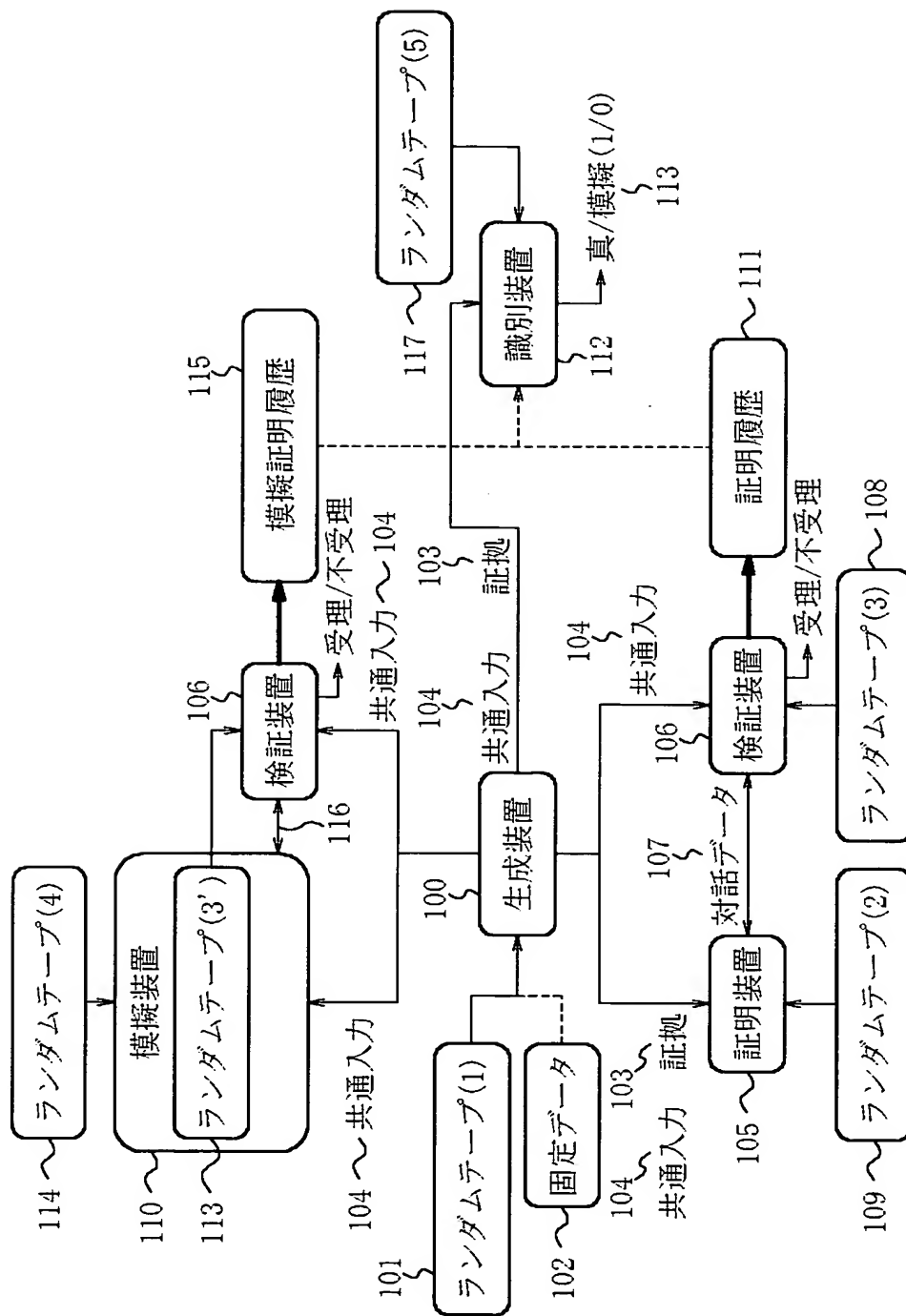
4 0 2 事例
4 0 3 ランダム事例生成装置 G R
4 0 4 ランダムテープ r G R
4 0 5 ランダムテープ r G P R
4 0 6 判別問題生成装置 G P R
5 0 0 生成装置
5 0 1 ランダムテープ r G
5 0 2 固定データ
5 0 3 証拠
5 0 4 共通入力
5 0 5 証明装置
5 0 6 検証装置
5 0 7 証明部
5 0 8 ハッシュ部
5 0 9 交換データ
5 1 1 検証部
5 1 2 ハッシュ部
5 1 5 ランダムテープ r P
6 0 5 改変証明装置
6 0 9 乱数
6 1 0 改変証明履歴
6 1 1 模擬改変証明履歴
6 1 2 模擬装置
6 1 3 識別装置
6 1 8 交換データ
7 0 2 生成装置
7 0 5 証拠
8 0 0 模擬装置
8 0 1 ランダムテープ r S

8 0 2	チャレンジ
8 0 3	リスポンス
8 0 8	証明履歴
9 0 0	ディフィーヘルマン事例生成装置 G D H
9 0 1	ランダム事例生成装置 G R
9 0 2	ランダムテープ r G D R
9 0 6	判別問題生成装置 G P R
9 0 7	証明履歴
9 0 8	証拠
9 1 0	チャレンジ
9 1 1	リスポンス
1 0 0 1	評価者端末
1 0 0 2	記憶装置
1 0 0 3	提示者端末
1 0 0 4	ネットワーク
1 0 0 5	記憶装置
1 0 0 7	被提示者端末
1 0 0 9	評価の根拠

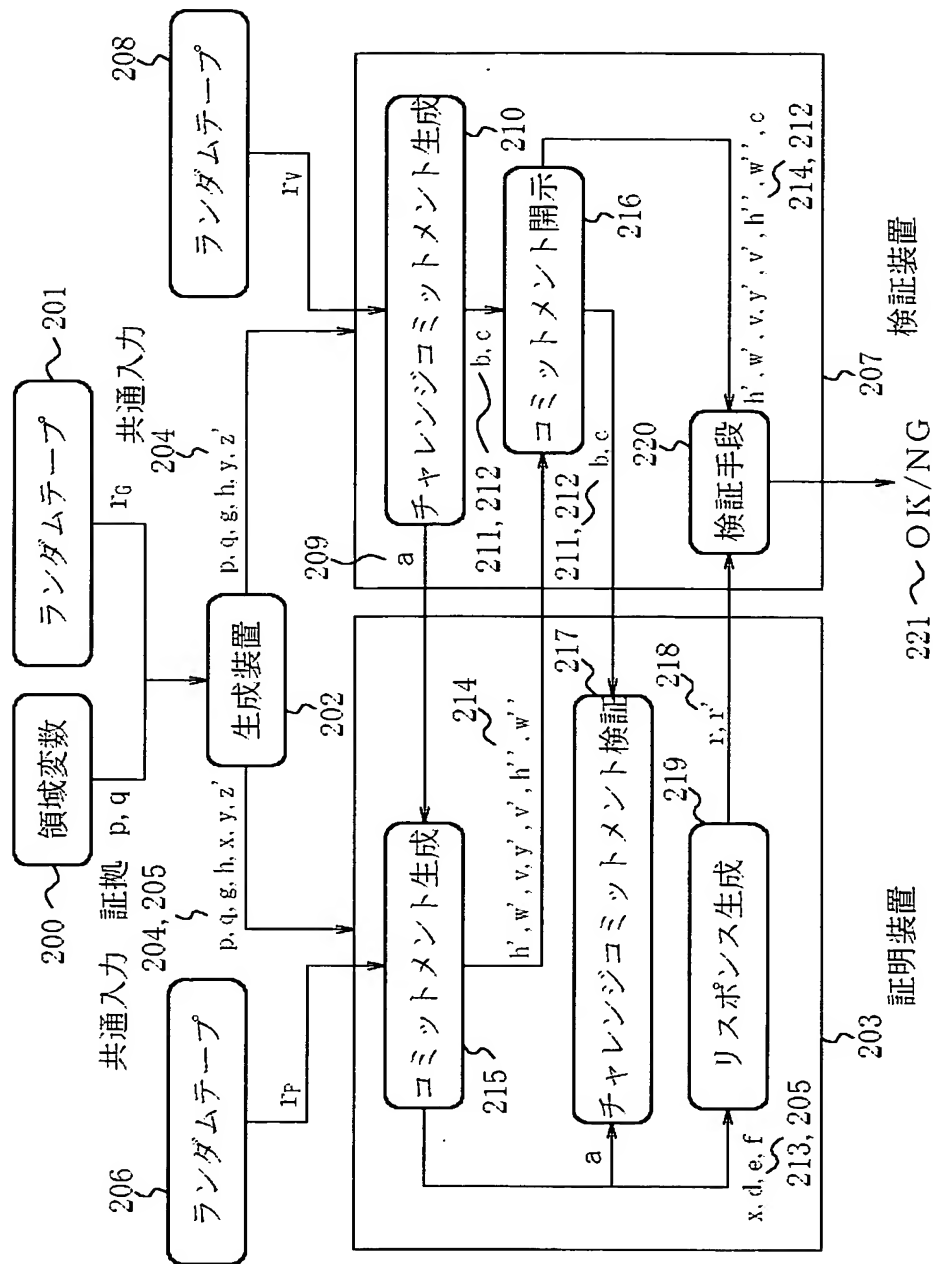
【書類名】

図面

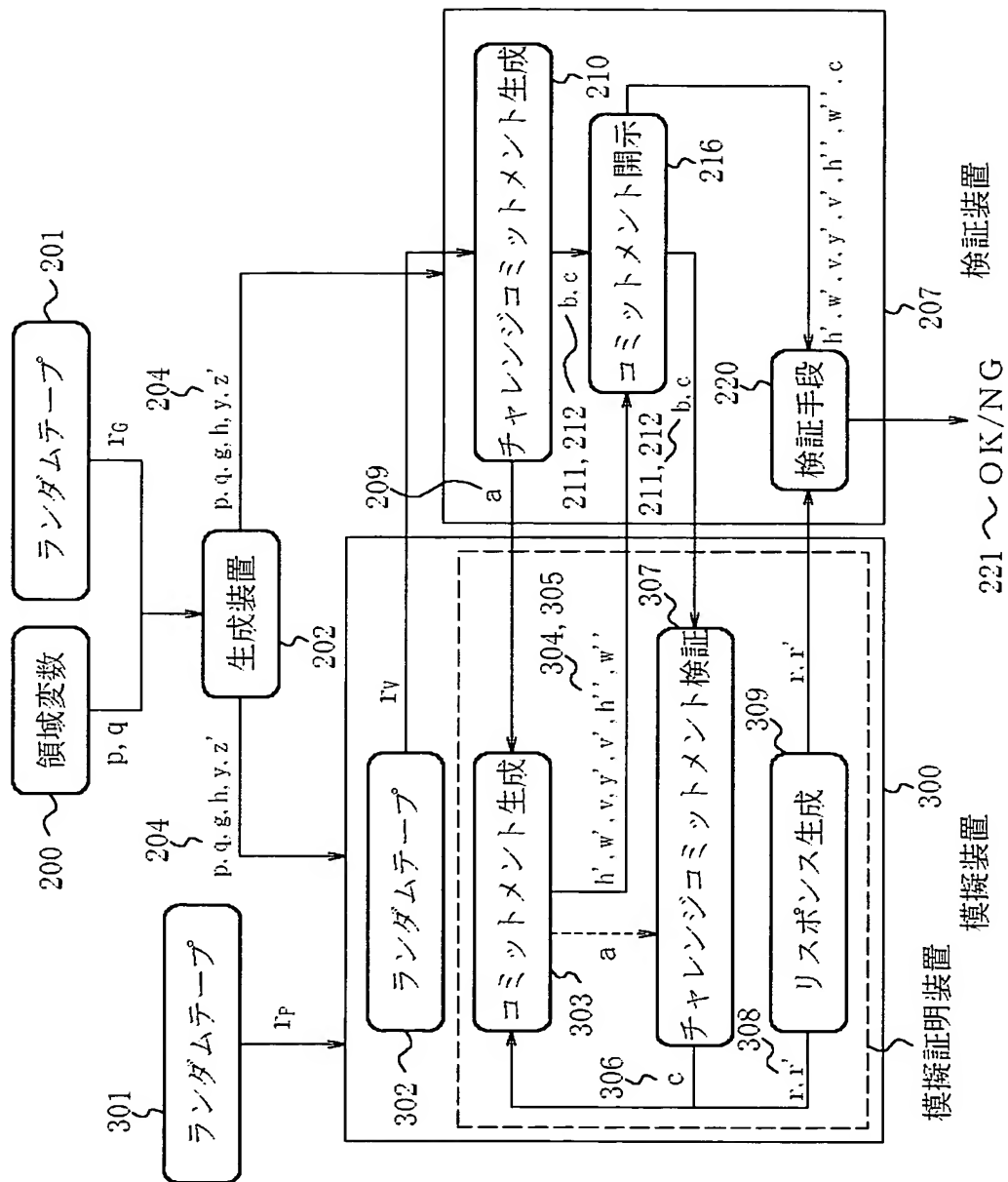
【図 1】



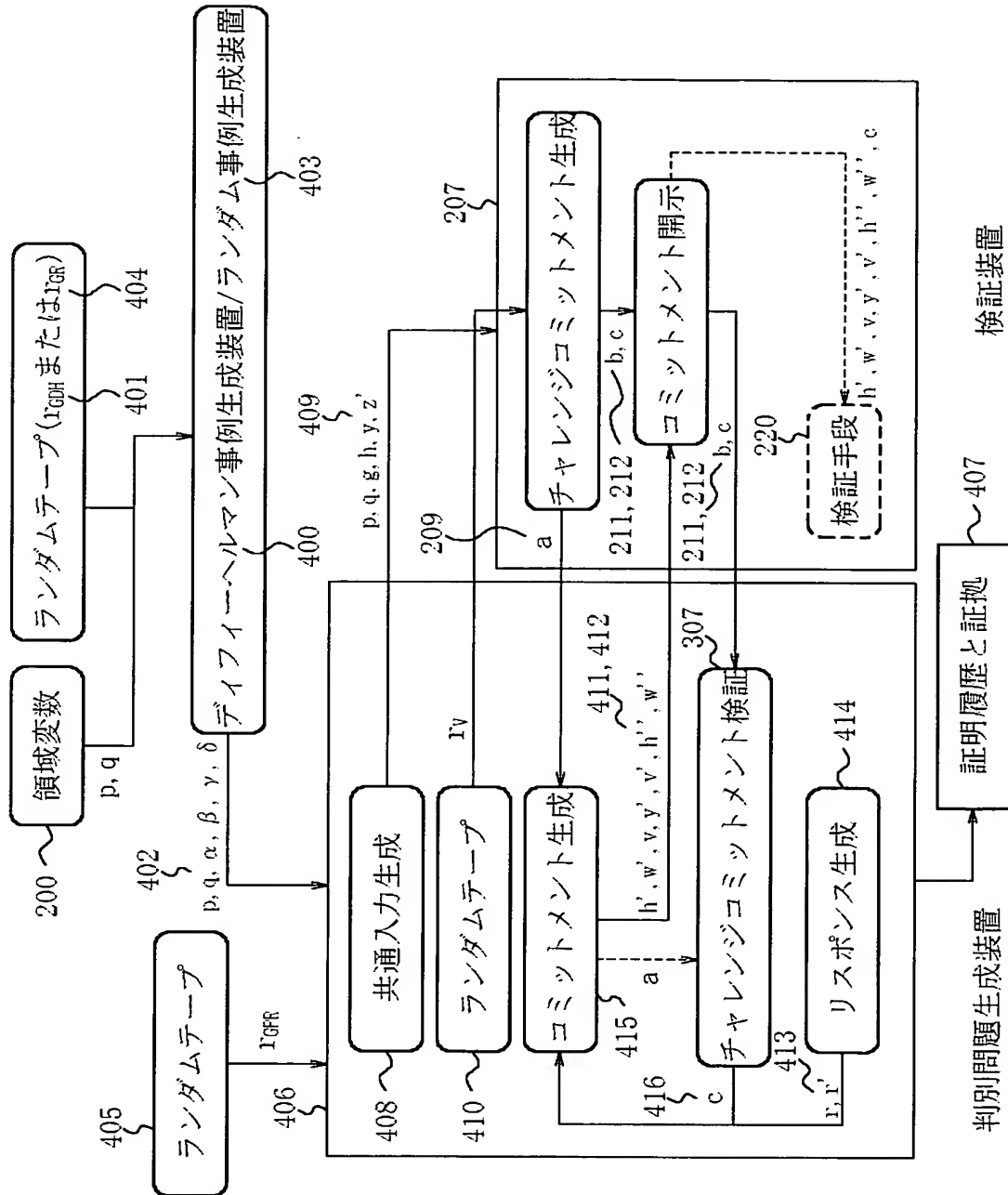
【図 2】



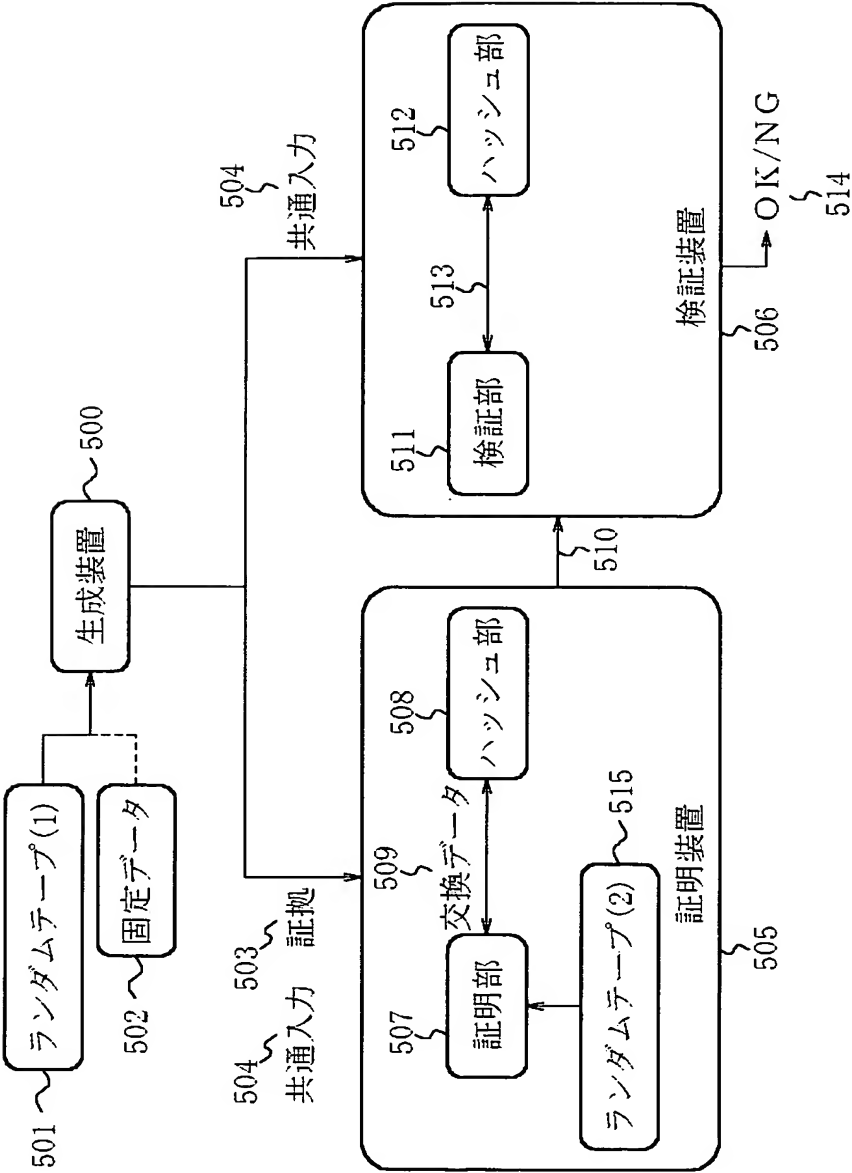
【図 3】



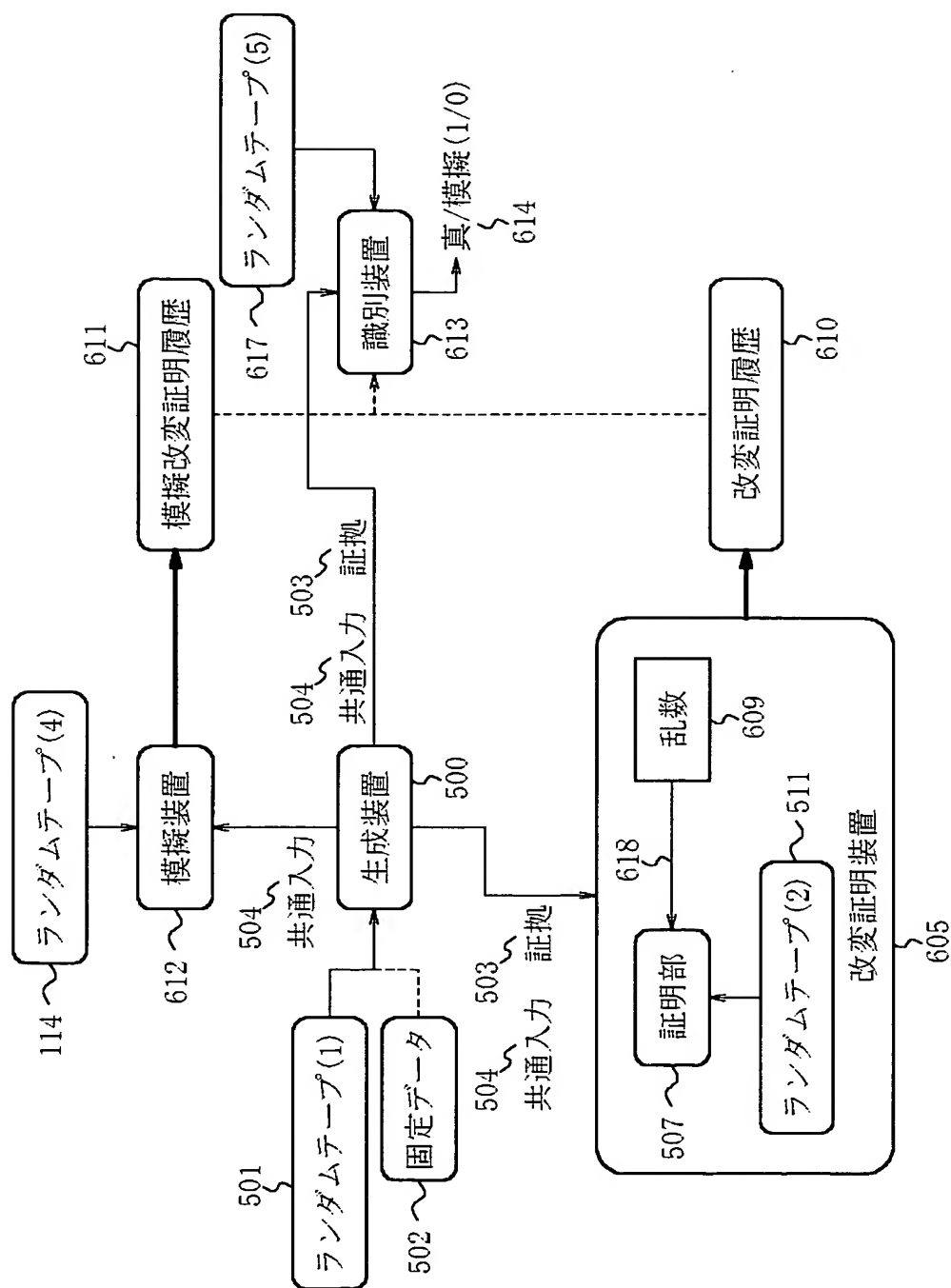
【図 4】



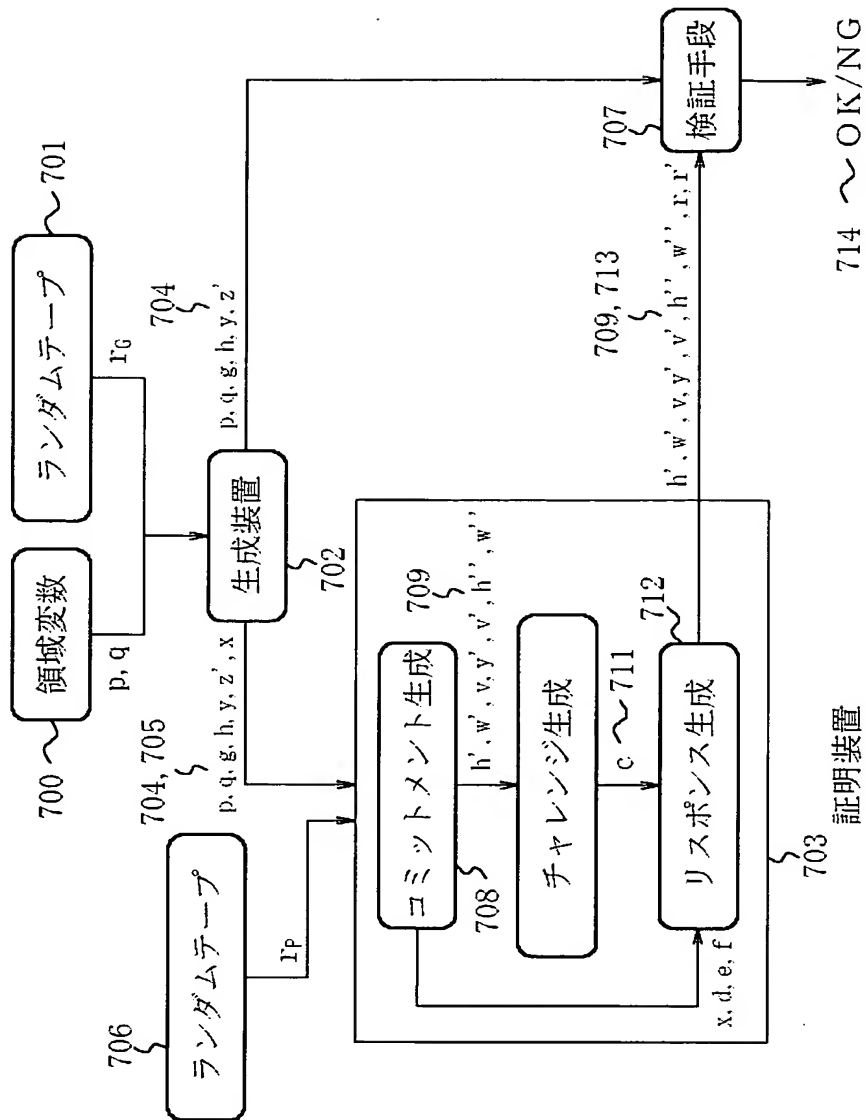
【図 5】



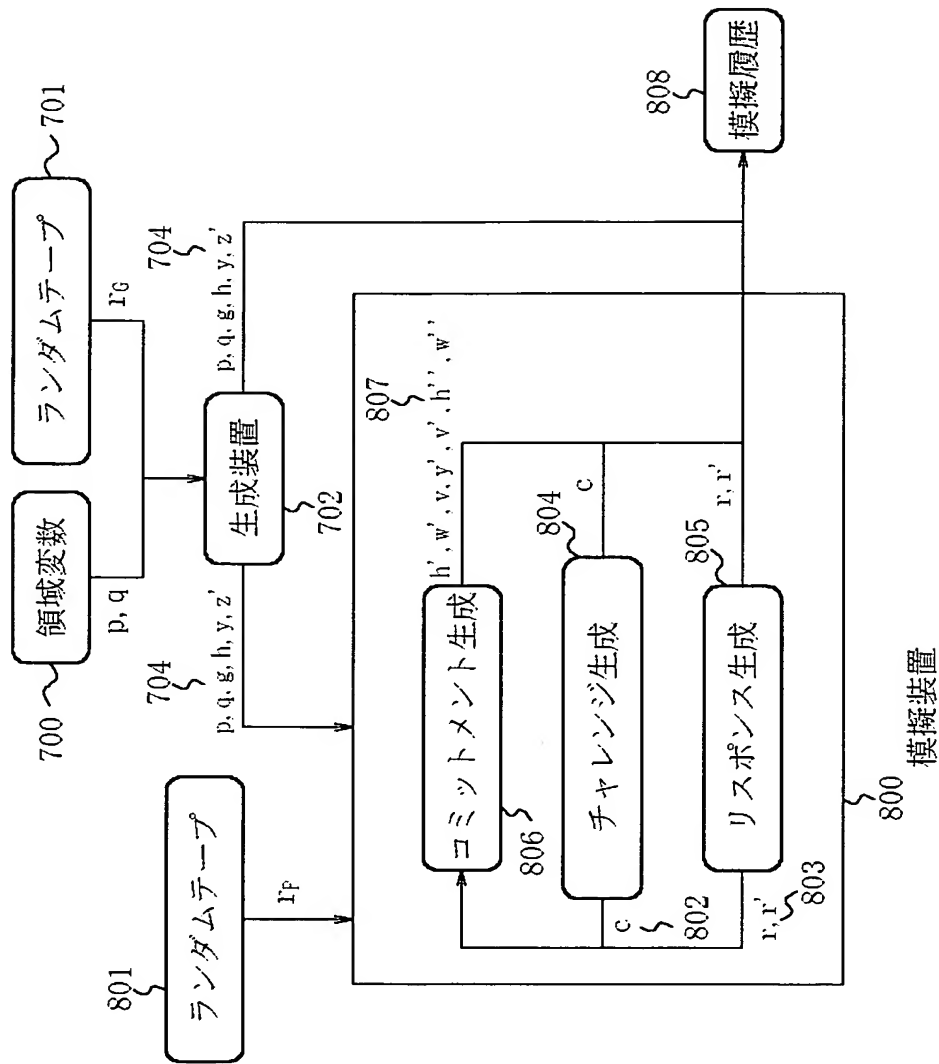
【図 6】



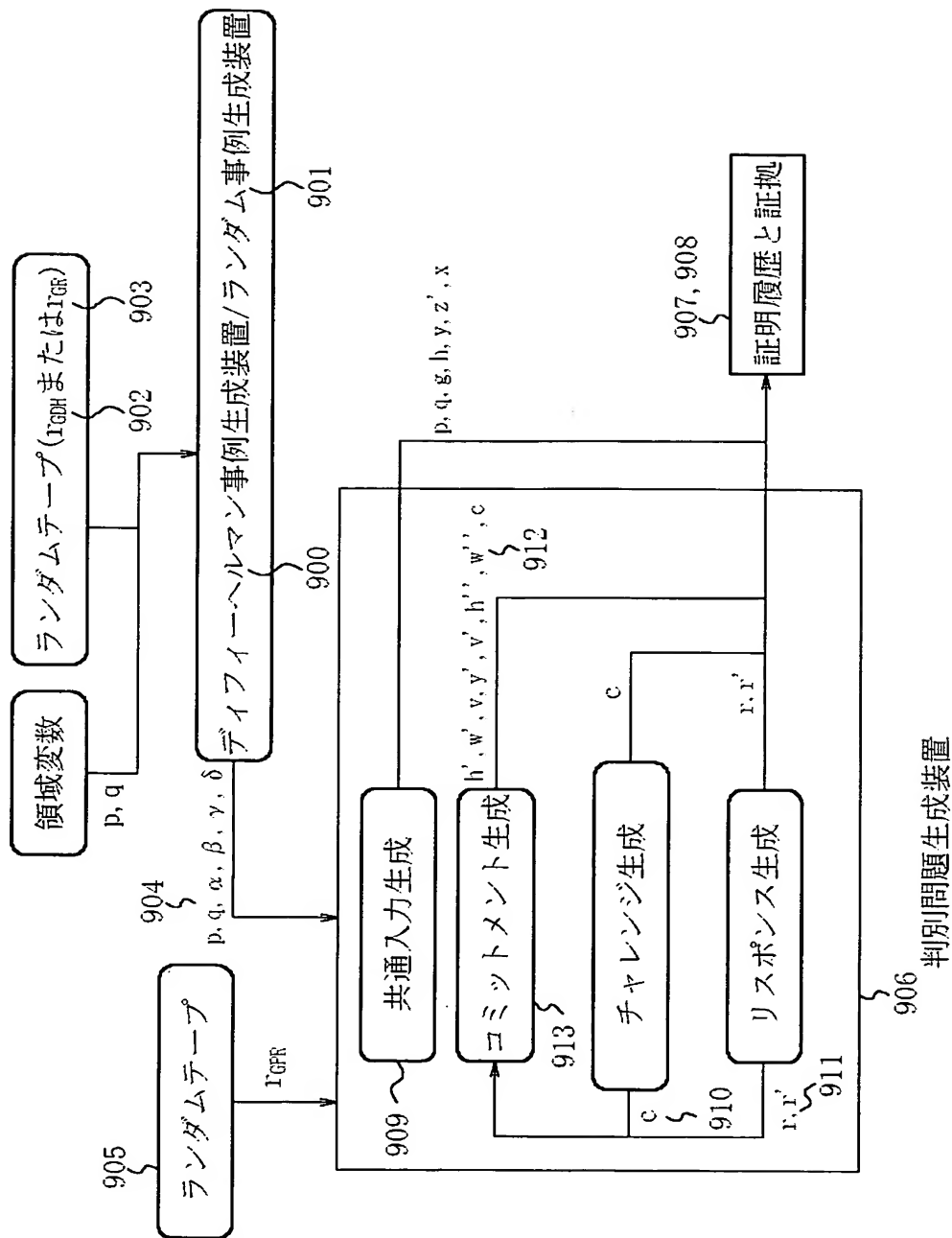
【図 7】



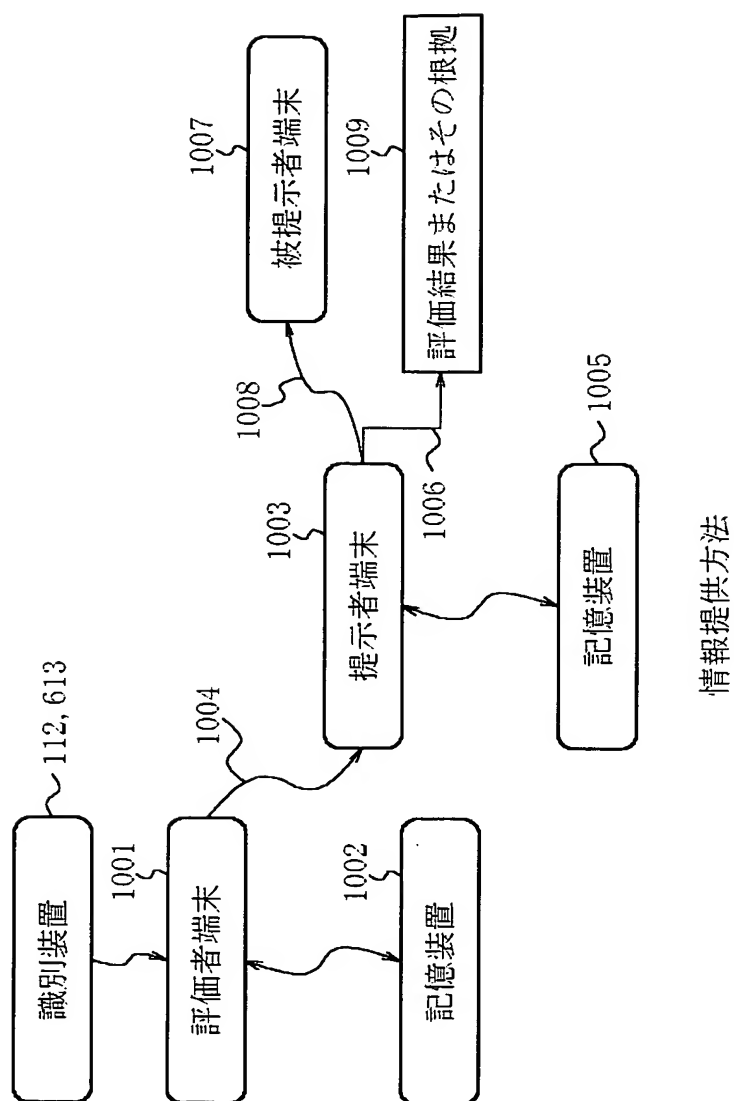
【図 8】



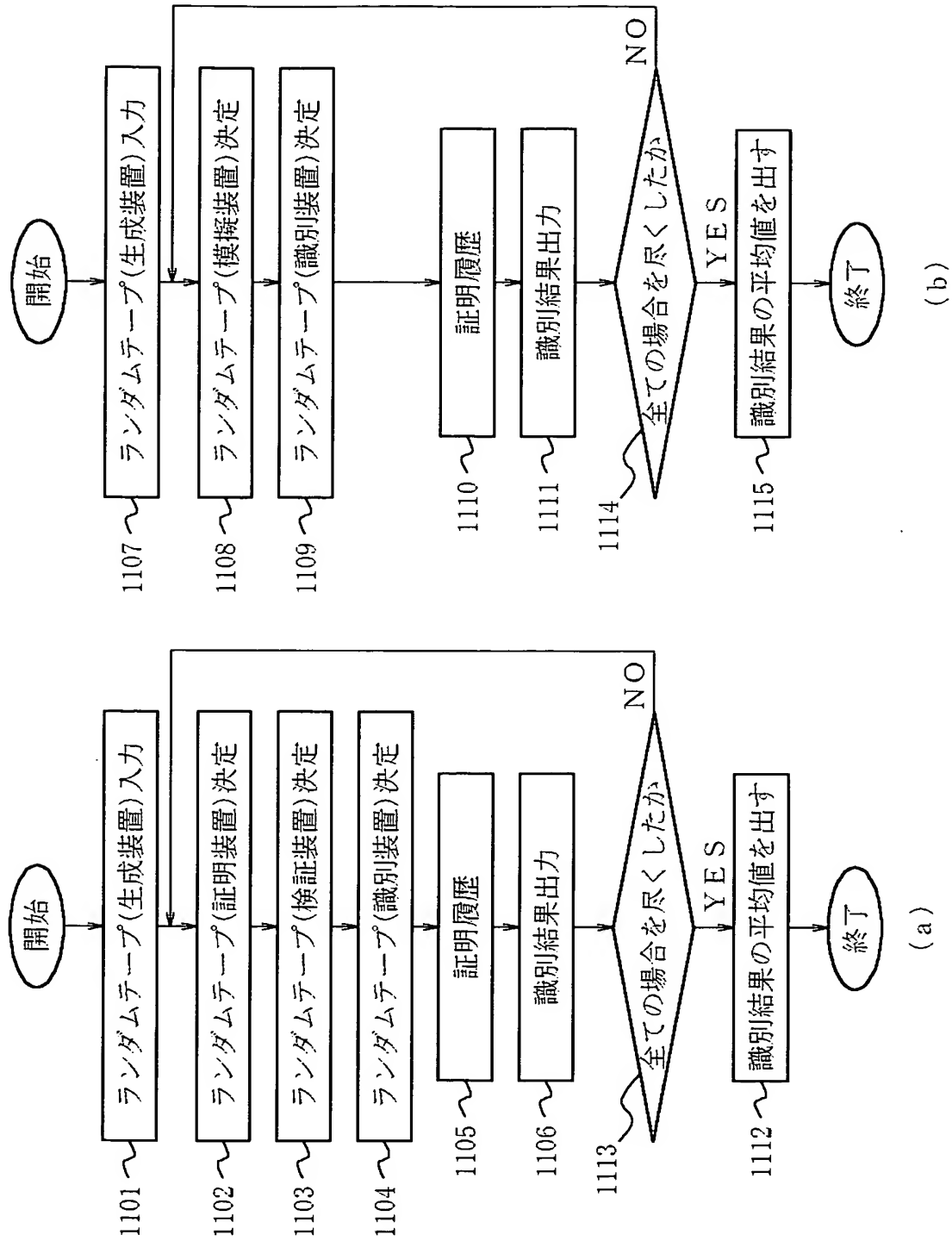
【図 9】



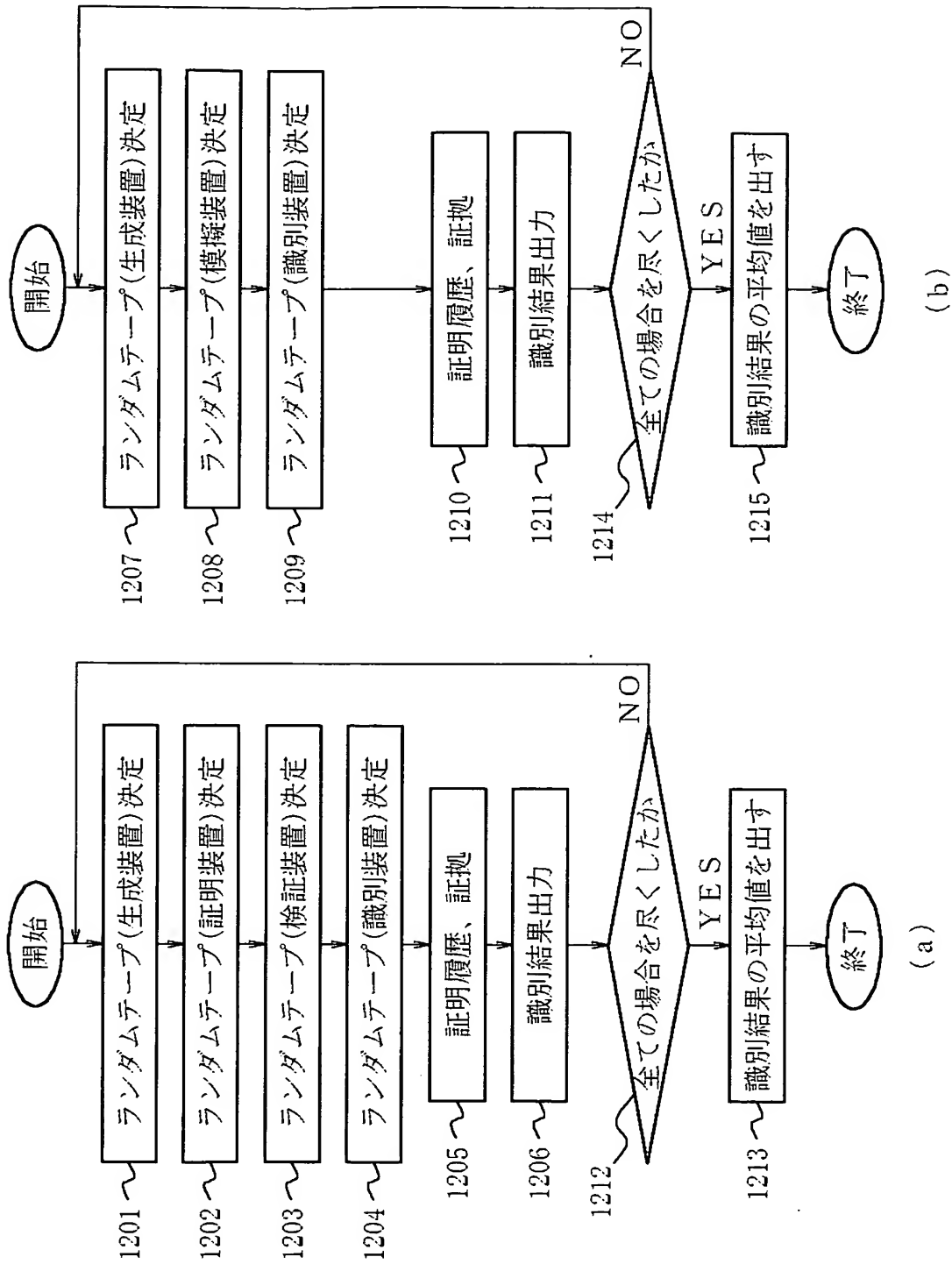
【図 10】



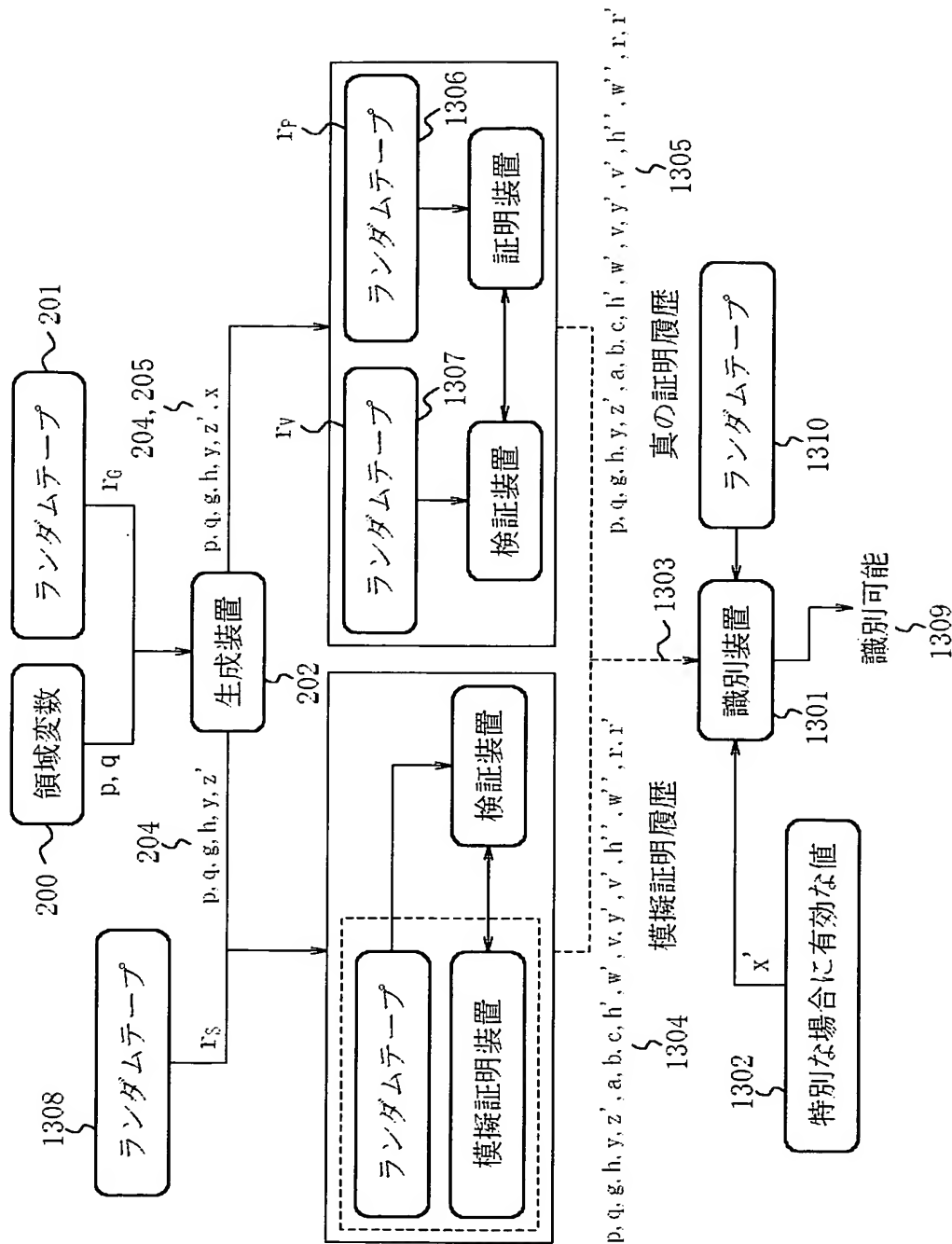
【図 11】



【図 12】



【図 13】



【書類名】 要約書

【要約】

【課題】 証明システムが零知識証明に属するための制約は厳しく、必ずしも所望の性質を満たす零知識証明を構成できるとは限らないという問題があった。

【解決手段】 本発明は、電子署名、公開鍵暗号、相手認証、メッセージ認証等の暗号プロトコルの基本技術である零知識証明を拡張したものであり、本発明が注目したのは、零知識証明であれば秘密の漏洩はないが、秘密の漏洩がなくても零知識証明であるとは限らないという事実である。この点に注目して、零知識証明よりも広い範囲の証明システムに対して、知識が漏れないことを保証できることを発見した。この発見を利用すれば、今まで零知識証明に属しなかった証明システムで、知識の漏がないことが保証されるものを利用すれば、今まで不可能であった所望の特徴を満たす証明システムが構成可能である場合が多々ある。このような証明システムが本発明の中心的な要素である。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2 0 0 2 - 3 4 1 1 1 2
受付番号	5 0 2 0 1 7 7 7 1 6 1
書類名	特許願
担当官	第七担当上席 0 0 9 6
作成日	平成 1 4 年 1 1 月 2 6 日

< 認定情報・付加情報 >

【提出日】	平成14年11月25日
-------	-------------

次頁無

特願 2 0 0 2 - 3 4 1 1 1 2

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 4 2 3 7]

1. 変更年月日

1 9 9 0 年 8 月 2 9 日

[変更理由]

新規登録

住 所

東京都港区芝五丁目 7 番 1 号

氏 名

日本電気株式会社